Jersey Financial Services Commission

Handbook for the prevention and detection of *money laundering*, the countering of *terrorist financing*, and the countering of *proliferation financing*

Note:

- *This Handbook* is applicable to all *supervised persons*. *Supervised persons* are described as 'relevant persons' in the *Money Laundering* (Jersey) Order 2008.
- The Handbook contains references to paraphrased Jersey *AML/CFT/CPF* legislation. Refer to our legislation pages for links to the full laws.
- Label references and colour-coding have been used to make the Handbook easier to navigate. The key below sets out which elements of the Handbook are mandatory, and which may be treated as guidance.
- If a term is defined in the Glossary, it appears in the Handbook in italic text.

We would strongly encourage you to seek independent advice to ensure your compliance with the regulatory framework.

Key:

The below table is applicable to sections 1-16 of *this Handbook*:

Section	Colour	Obligation explained
Section heading	**Blue**	Relates to all *supervised persons* (except *Prescribed NPOs*).
Subheading	**Grey**	Relates to all *supervised persons* (except *Prescribed NPOs*).
Statutory requirements	**Light blue**	Mandatory for all *supervised persons* (except *Prescribed NPOs*).
AML/CFT/CPF Codes of Practice	**Magenta**	Mandatory for all *supervised persons* (except *Prescribed NPOs*).
Guidance notes	**Green**	Guidance for all *supervised persons* (except *Prescribed NPOs*).

PART I: GENERAL GUIDANCE [sections 1 – 11]: applicable to all entities/sectors classified as *supervised persons* (except prescribed *NPOs*).

PART II: SECTOR SPECIFIC GUIDANCE [sections 12 – 16]: applicable to those sectors as noted in the relevant sections.

PART III: DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONALS (*DNFBPS*) [sections 17 – 21]: Specific guidance for *DNFBPs* including introduction relevant for all *DNFBPs*.

PART IV: GLOSSARY [section 22]: Key terms.

For example, a *DNFBP* as outlined by Schedule 2 of the *Proceeds of Crime Law* would find applicable guidance in Part I (sections 1 – 11) and Part III (section 17 and the specific applicable *DNFBP* section).

For help with navigation, chat with Reggie, the JFSC regulatory chatbot.

Contents

Part I: GENERAL GUIDANCE

1 INTRODUCTION

1. The continuing ability of Jersey's finance industry to attract legitimate *customers* with funds and assets that are clean and untainted by criminality depends, in large part, upon the Island's reputation as a sound, well-regulated jurisdiction. Any business that assists in *money laundering*, the *financing of terrorism*, or the *financing of proliferation*, whether:

› with knowledge or suspicion of the connection to crime; or

› acting without regard to what it may be facilitating through the provision of its products or services;

will face the loss of its reputation, risk the loss of its *Licence* or other regulatory sanctions (where regulated and supervised), damage the integrity of Jersey's finance industry, and may risk prosecution for criminal offences.

2. Jersey has had in place a framework of *AML* legislation since 1988, and for the *CFT* since 1990. This legislation has continued to be updated as new threats have emerged, including legislation to extend the definition of criminal conduct for which a *money laundering* offence can be committed and to combat international terrorism.

3. Criminals are aware of the *AML/CFT/CPF* measures taken by the traditional financial sector over the past decade and may seek other means to convert their proceeds of crime, or to mix them with legitimate income before they enter the banking system, thus making them harder to detect. *Lawyers*, *Trust Company Businesses* and providers of *accountancy services* have all been used as a conduit for criminal property to enter the financial system and are sometimes referred to as "gatekeepers". Some have also been used to assist terrorists and proliferators of weapons of mass destruction to plan and finance their operations.

4. For example, criminals may try to exploit the services offered by *Lawyers*, through the business of undertaking property and financial transactions, setting up corporate and trust structures and when acting as directors or trustees. In addition, client accounts can provide a money launderer with a route into the banking system.

5. The result has been that international *AML/CFT/CPF* legislation and standards have been extended beyond the traditional financial sector to all *supervised businesses*. *This Handbook* applies to all *supervised persons* (throughout *this Handbook*, where provisions of the *Money Laundering Order* are quoted, paraphrased, or summarised, the text refers to a *relevant person* to match the language of the *Money Laundering Order*).

6. Jersey's defences against *money laundering*, the *financing of terrorism*, and *financing of proliferation* rely heavily on the vigilance and co-operation of the finance sector. *The Money Laundering Order* is therefore also in place covering *supervised persons*.

7. The primary legislation is defined in the Glossary of *this Handbook* as the *Anti-Money Laundering and Counter-Terrorism Legislation*.

8. The international standards require that all *Financial Institutions, DNFBPs* and *VASPs* must be supervised on a risk-based approach by an appropriate *AML* supervisory body. Within Jersey, the *JFSC* has been designated as the relevant supervisory body under the *Supervisory Bodies Law*. The *JFSC* is the *AML/CFT/CPF* supervisor for all *supervised persons*. Ensuring compliance and acting against those that do not comply with the measures to guard against *money laundering, t*he *financing of terrorism*, and the *financing of proliferation*, is crucial to the effectiveness of Jersey's preventative regime.

9. *Supervised persons* may get a visit from the *JFSC* to carry out an examination. Further information related to this can be found on the *JFSC's* website. In certain circumstances, the *JFSC* may also serve a notice on a *supervised person* which would require, among other things, senior management to attend interviews and to answer questions and/or provide information and documents.

10. Each *supervised person* in Jersey must recognise the role that it must play in protecting itself, and its *employees*, from involvement in *money laundering*, the *financing of terrorism*, and the *financing of proliferation*, and in protecting the Island's reputation. This relates not only to business operations within Jersey, but also operations conducted by *supervised persons* outside the island.

11. The *JFSC* strongly believes that the key to the prevention and detection of *money laundering*, the *financing of terrorism*, and the *financing of proliferation* lies in the implementation of, and strict adherence to, effective *systems and controls*, including sound *CDD* measures based on international standards. The *AML/CFT/CPF Handbook* therefore establishes standards which match international standards issued by the *FATF*. *This Handbook* also has regard to the standards promoted by the Basel Committee, *IOSCO* and the *IAIS*. The *Handbook* takes account of the requirements of EU legislation to counter *money laundering*, the *financing of terrorism*, and the *financing of proliferation* and its application of standards set by the *FATF*.

12. The *JFSC* is also mindful of the importance of financial services being generally available to all Jersey residents and, where necessary, *this Handbook* incorporates measures to guard against the financial exclusion of Jersey residents from financial services and products.

13. Throughout *this Handbook*, *supervised persons* should have regard to the defined terms set out in the Glossary of *this Handbook*.

1.1 *Guidelines*

14. The *Handbook* applies to *supervised persons* whose activities and/or operations are within the specified list of activities in Schedule 2 of the *Proceeds of Crime Law* that are *financial services business.*

15. *Guidelines,* that are published on the *JFSC* website, provide guidance on interpretation of provisions and expressions relating to the list of activities and operations constituting *financial services business* including what is meant by "when conducted as a business". The *Guidelines* assist entities in determining whether their activities and operations are within scope of the *statutory requirements.* Account must also be taken of the *FATF Recommendations,* particularly where the same expressions are used.

1.2 Objectives of the *AML/CFT/CPF Handbook*

16. The objectives of *this Handbook* are:

› to outline the relevant requirements of the *Anti-Money Laundering and Counter-Terrorism Legislation*;

- to set out the *JFSC's* requirements, expressed as *AML/CFT/CPF Codes of Practice* - to be followed by all *supervised persons*;
- to assist *supervised person*s to comply with the requirements of the *Anti-Money Laundering and Counter-Terrorism Legislation* and the *AML/CFT/CPF Codes of Practice*, through practical interpretation;
- to outline good practice in developing *systems and controls* to prevent *supervised persons* from being used to facilitate *money laundering*, the *financing of terrorism*, and the *financing of proliferation;*
- to provide a base from which *supervised persons* can design and implement *systems and controls* and tailor their own *policies and procedures* for the prevention and detection of *money laundering,* the *financing of terrorism*, and the *financing of proliferation* (and which may also help to highlight identity fraud);
- to ensure that Jersey matches international standards to prevent and detect *money laundering*, the *financing of terrorism*, and the *financing of proliferation;*
- to provide direction on applying the risk-based approach effectively;
- to provide more practical guidance on applying *CDD* measures, including finding out identity and obtaining evidence of identity;
- to emphasise the responsibilities of the board and senior management of a *supervised person* in preventing and detecting *money laundering*, the *financing of terrorism*, and the *financing of proliferation*;
- to promote the use of a proportionate, risk-based approach to *CDD* measures, which directs resources towards higher risk *customers*;
- to emphasise the particular *money laundering*, the *financing of terrorism*, *and* the *financing of proliferation* risks of certain financial services and products;
- to provide an information resource to be used in training and raising awareness of *money laundering*, the *financing of terrorism*, and the *financing of proliferation*.

17. *This Handbook* will be reviewed on a regular basis and, where necessary following consultation, amended considering experience, changes in legislation, and the development of international standards.

18. *This Handbook* is intended to be used by senior management and compliance staff in the development of a *supervised person's systems and controls*, and detailed *policies and procedures*. Each *supervised person* is expected to draw up its own *policies and procedures* based on the guidance set out in the *Handbook*. These *policies and procedures* will also help senior management and staff to comply with their own personal obligations under the *Anti-Money Laundering and Counter-Terrorism Legislation*. *This Handbook* is not intended to be used by *supervised persons* as an internal *procedures'* manual.

19. *Supervised persons* are expected to think about how they might be vulnerable to and exploited by criminals. The *Anti-Money Laundering and Counter-Terrorism Legislation* expects *supervised persons* to manage the risks of being used by criminals, *terrorists,* or *proliferators* of weapons of mass destruction, and to document how they are managing those risks.

20. **All *supervised persons*** should have regard to the main sections of *this Handbook* (Sections 1-11). *Supervised persons* should also refer to the sector-specific sections of *this Handbook* (Sections 12-21) relevant to their type of business when drawing up their *policies and procedures*.

1.3 Structure of the *AML/CFT/CPF Handbook*

21. *This Handbook* describes *statutory requirements* (defined below), sets out principles and detailed requirements (*AML/CFT/CPF Codes of Practice*), and presents ways of complying with *statutory requirements* and the *AML/CFT/CPF Codes of Practice* (G*uidance notes*).

22. *Statutory requirements* describe the statutory provisions that must be complied with by a *supervised person* (natural or legal) when carrying on a *supervised business*, in particular requirements set out in the *Money Laundering Order*. Some *statutory requirements* place obligations on individuals. Failure to follow a *Statutory Requirement* is a criminal offence and may also attract regulatory sanction.

23. The *AML/CFT/CPF Codes of Practice* set out principles and detailed requirements for compliance with *statutory requirements,* failure to follow any *AML/CFT/CPF Codes of Practice* may attract regulatory sanction. The *AML/CFT/CPF Codes of Practice* comprise several individual elements:

› to be followed in the area of corporate governance, which must be in place in order for a *supervised person* to comply with *statutory requirements*; and

› explain in more detail how a s*tatutory requirement* is to be complied with.

24. *Guidance notes* present ways of complying with the *statutory requirements* and *AML/CFT/CPF Codes of Practice* and must always be read in conjunction with these. A *supervised person* may adopt other measures to those set out in the G*uidance notes*, including *policies and procedures* established by a group that it is part of, so long as it can demonstrate that such measures also achieve compliance with the *statutory requirements* and *AML/CFT/CPF Codes of Practice*. This allows a *supervised person* discretion as to how to apply requirements in the particular circumstances of its business, products, services, transactions, and *customers*. The soundly reasoned application of the provisions contained within the *Guidance notes* will provide a good indication that a *supervised person* is in compliance with the s*tatutory requirements* and *AML/CFT/CPF Codes of Practice*.

25. The provisions of the *statutory requirements* and of the *AML/CFT/CPF Codes of Practice* are described using the term **must**, indicating that these requirements are mandatory. However, in exceptional circumstances, where strict adherence to any of the *AML/CFT/CPF Codes of Practice* would produce an anomalous result, a *supervised person* may apply in advance in writing to the *JFSC* for a variance from the requirement. Section 1.9 of *this Handbook* also explains that an obligation to do something outside Jersey may be met through applying measures that are at least equivalent to the *AML/CFT/CPF Codes of Practice*.

26. In contrast, the *Guidance notes* use the term **may**, indicating ways in which the requirements may be satisfied, but allowing for alternative means of meeting the *statutory requirements* or *AML/CFT/CPF Codes of Practice*.

27. *This Handbook* also contains **Overview** text which provides context relevant to particular sections or sub-sections of the *AML/CFT/CPF Handbook*.

28. *This Handbook* is not intended to provide an exhaustive list of *systems and controls* to counter *money laundering*, the *financing of terrorism*, and the *financing of proliferation*. In complying with the *statutory requirements* and *AML/CFT/CPF Codes of Practice*, and in applying the G*uidance notes*, a *supervised person* should (where permitted) adopt an appropriate risk-based approach and should always consider what additional measures might be necessary to prevent its exploitation, and that of its products and services, by persons seeking to engage in *money laundering*, the *financing of terrorism*, *and* the *financing of proliferation*.

29. The text in *statutory requirements* sections necessarily paraphrases provisions contained in the *Anti-Money Laundering and Counter-Terrorism Legislation* and should always be read and understood in conjunction with the full text of each law. *Statutory requirements* are presented in light blue boxes and in italics, to distinguish them from other text.

1.4 Legal status and sanctions for non-compliance

1.4.1 *AML/CFT/CPF Handbook*

30. *This Handbook* is issued by the *JFSC*:

› pursuant to its powers under Article 8 of the *Commission Law;*

› in accordance with Article 22 of the *Supervisory Bodies Law*, which provides for *Codes of Practice* to be prepared and issued for the purpose of setting out principles and detailed requirements;

› in light of the *Proceeds of Crime Law*, which provides for the *Money Laundering Order*;

› in Article 37 (1) (a) of the *Proceeds of Crime Law,* the Chief *Minister* must prescribe measures to be taken (or not to be taken) by persons who carry on *financial services business*; and

› in Article 37 (1) (c) of the *Proceeds of Crime Law,* the Chief *Minister* may prescribe measures to be taken by persons or categories of persons appointed for the purposes of fulfilling the obligations prescribed in respect of persons referred to in Article 37 (1) (a).

31. The *AML/CFT/CPF Codes of Practice* in *this Handbook* are applicable to **all *supervised persons*.**

32. Sector-specific sections for *supervised persons* subject to the funds, security issuers and their service providers, *TCSPs, Wire Transfers Regulations, prepaid cards, AMLSPs, VASPs, real estate agents, high value dealers, Lawyers and Accountants* are set out at Sections 12-21 of *this Handbook* and provide some additional *AML/CFT/CPF Codes of Practice* and *Guidance notes* for *supervised persons* carrying on those types of business.

1.4.2 *Money Laundering Order*

33. The *Money Laundering Order* is made by the *Minister* for External Relations and Financial Services under Article 37(1)(a) of the *Proceeds of Crime Law*. The *Money Laundering Order* prescribes measures to be taken (including measures not to be taken) by a *relevant person* for the purposes of preventing and detecting *money laundering,* the *financing of terrorism* and *proliferation financing*.

34. Article 37 (1)(b) of the *Proceeds of Crime Law* provides, where applicable, for a *relevant person* to appoint persons or categories of persons for the purpose of fulfilling the obligations of the *relevant person* (see section 18 *of this Handbook*).

35. Failure to comply with the *Money Laundering Order* is a criminal offence under Article 37(4) of the *Proceeds of Crime Law*. In determining whether a *supervised person* has complied with any of the requirements of the *Money Laundering Order*, the Royal Court is, pursuant to Article 37(8) of the *Proceeds of Crime Law*, required to take account of the *AML/CFT/CPF Codes of Practice* and G*uidance notes* issued by the *JFSC*, as amended from time-to-time.

36. The sanction for failing to comply with the *Money Laundering Order* may be an unlimited fine or up to two years imprisonment, or both.

37. Under Article 39A(2) of the *Proceeds of Crime Law*, if a ‘relevant offence’ is proved to have been committed by a *financial services business* with the consent or connivance of a ‘*relevant person*’ (both as defined in Article 39A(1) of that law) that ‘*relevant person*’ is also guilty of the offence and liable to the same penalty for that offence as the *financial services business*.

38. Under Article 35A of the *Proceeds of Crime Law*, a *financial services business* commits an offence if a person is engaged in *money laundering* when acting in the capacity of a person associated with that business (as defined in Article 35A(4) of the *Proceeds of Crime Law*).

39. If the *financial services business* is a body corporate, it is liable to a fine. If the business is not a body corporate, they are liable to imprisonment for a term not exceeding two years or to a fine, or to both.

40. In determining whether a person has committed an offence under Article 21 of the *Terrorism Law* (the offence of failing to report), the Royal Court is, pursuant to Article 21(6) of the *Terrorism Law*, required to take account of any guidance provided (for this purpose guidance will include the *AML/CFT/CPF Codes of Practice* read in conjunction with the overview text and the *Guidance notes*), as amended from time-to-time. The sanction for failing to comply with Article 21 of the *Terrorism Law* may be an unlimited fine or up to five years imprisonment, or both.

41. It should be emphasised that *this Handbook* is not a substitute for the law and compliance with it is not of itself a defence to offences under the various legislation referenced above. However, *the Handbook* shall be considered by the courts when considering the standards of a *supervised person’s* conduct and whether they acted reasonably, honestly, and appropriately, and took all reasonable steps and exercised necessary due diligence to avoid committing the offence.

42. Under Article 21A of the *Commission Law* the *JFSC* may impose a civil financial penalty on a *supervised person* (except where that person is a fund) where the *JFSC* is satisfied that the *supervised person* has, to a significant and material extent, contravened the *Money Laundering Order*.

43. Article 21A of the *Commission Law* also permits the *JFSC* to impose a civil financial penalty on a principal person, a key person or a person who performs or performed a senior management function (all as defined in Article 1 of the *Commission Law*) where the *JFSC* is satisfied that the contravention of the *Money Laundering Order* by the *supervised person* was:

› committed with the consent or connivance of, or is attributable to neglect on the part of, the principal person, key person or the person who performs or performed a senior management function; or

› aided, abetted, counselled, or procured by such a person.

44. The *JFSC* has published a notice designating “senior management functions” on its website – effective from 13 March 2023.

1.4.3 AML/CFT/CPF *Codes of Practice*

45. The *AML/CFT/CPF Codes of Practice* are prepared and issued by the *JFSC* under Article 22 of the *Supervisory Bodies Law*. The *AML/CFT/CPF Codes of Practice* set out the principles and detailed requirements that must be complied with to meet certain *statutory provisions* of the *Supervisory Bodies Law* and the *Anti-Money Laundering and Counter-Terrorism Legislation (Proceeds of Crime Law*, *Terrorism Law*, *Directions Law*, *Targeted Financial Sanctions Measures*, *Wire Transfers Regulations*, and the *Money Laundering Order)* by *supervised persons*. The *AML/CFT/CPF Codes of Practice* comprise several individual *AML/CFT/CPF Codes of Practice.*

46. Article 5 of the *Supervisory Bodies Law* states that the *JFSC* shall be the supervisory body to exercise supervisory functions in respect of a *regulated person (*as defined in Article 1 of the *Supervisory Bodies* Law). The *JFSC* is also designated under Article 6 of the *Supervisory Bodies Law* to exercise supervisory functions in respect of any other person carrying on a *supervised business*. The effect of these provisions is to give the *JFSC* supervisory functions in respect of all *supervised persons*.

47. Article 8A of the *Supervisory Bodies Law* requires a supervisory body (i.e., the *JFSC*) to use a risk-based approach when performing its obligations under said law, which means determining the scrutiny that a *supervised person* requires based on:

- the *money laundering* and *terrorist financing* risks associated with the *supervised person*, as identified by the supervisory body's assessment of the *supervised person's* risk profile;
- the policies, internal controls and procedures associated with the *supervised person*, as identified by the supervisory body's assessment of the *supervised person's* risk profile;
- the *money laundering* or *terrorist financing* risks present in the jurisdiction in which the *supervised person* is based;
- any other characteristic of the *supervised person* that the supervisory body reasonably considers to be relevant.

48. Article 8A(3) of the *Supervisory Bodies Law* requires the supervisory body (i.e. the *JFSC*) to take account of *FATF Recommendations* when devising a risk profile for a *supervised person*.

49. Compliance with the *AML/CFT/CPF Codes of Practice* will be considered by the *JFSC* in the conduct of its *supervisory programme*, including on-site examinations.

50. The consequences of non-compliance with any *AML/CFT/CPF Codes of Practice* could include an investigation by or on behalf of the *JFSC* and the imposition of regulatory sanctions. Regulatory sanctions available to the *JFSC* under the *Supervisory Bodies Law* and the *Regulatory Laws* (where applicable) include:

- issuing a public statement;
- imposing a registration condition;
- objecting to the appointment, or continued appointment, of a principal person (or equivalent controller or manager of a *regulated person*) or key person;
- imposing a direction and making this public, including preventing an individual from working in a *supervised person* and where already appointed requiring their removal; and
- revoking a *supervised person's* registration.

51. In addition, under Article 21A of the *Commission Law* the *JFSC* may impose a civil financial penalty on a *supervised person* (except where that person is a fund) where the *JFSC* is satisfied that the *supervised person* has, to a significant and material extent, contravened an *AML/CFT/CPF Code of Practice*.

52. Article 21A of the *Commission Law* also permits the *JFSC* to impose a civil financial penalty on a principal person, a key person or a person who performs or performed a senior management function (all as defined in Article 1 of the *Commission Law*) where the *JFSC* is satisfied that the contravention of the *AML/CFT/CPF Code of Practice* by the *supervised person* was:

- committed with the consent or connivance of, or is attributable to neglect on the part of, the principal person, key person or the person who performs or performed a senior management function; or
- aided, abetted, counselled, or procured by such a person.

53. The *JFSC* has published a notice designating "senior management functions" on its website – effective from 13 March 2023.

54. The ability of a *supervised person* to demonstrate compliance with *AML/CFT/CPF Codes of Practice* will also be directly relevant to its regulated status and any assessment of fitness and propriety of its *principal persons* and *key persons*. Non-compliance with any *AML/CFT/CPF Code of Practice* may be regarded by the *JFSC* as an indication of:

- a lack of fitness and propriety under Articles 7 or 8B of the *CIF(J) Law*, Article 10 of the *BB(J) Law*, Article 7 of the *IB(J) Law*, and Article 9 of the *FS(J) Law*; and/or
- a failure to follow certain fundamental principles within a Code of Practice issued under each of the *Regulatory Laws*.

55. Where a breach of an *AML/CFT/CPF Code of Practice* results in a contravention of the *Money Laundering Order*, a *supervised person* and its *employees* can be criminally prosecuted.

1.5 Jurisdictional scope of the *Money Laundering Order* and *AML/CFT/CPF Codes of Practice*

1.5.1 Application of the *Money Laundering Order* and *AML/CFT/CPF Codes of Practice* to *supervised persons* carrying on business in Jersey

56. By virtue of the definition of *relevant person* in Article 1(1), the *Money Laundering Order* applies to **any *supervised person*** who is carrying on a *supervised business* in or from within Jersey. This will include Jersey-based branches of companies incorporated outside Jersey conducting *supervised business* in Jersey.

57. A distinction should be made between a Schedule 2 business and a *Prescribed NPO*. Although both are *supervised persons*, *Prescribed NPOs* are not Schedule 2 businesses, and therefore are not subject to the requirements of the *Money Laundering Order*.

58. By virtue of Articles 5, 6 and 22 of the *Supervisory Bodies Law*, the *AML/CFT/CPF Codes of Practice* apply to **any *supervised person*** who is carrying on a *supervised business* in or from within Jersey. This will include Jersey-based branches of companies incorporated outside Jersey conducting *supervised business* in Jersey.

59. The *AML/CFT/CPF Codes of Practice* in Sections 2 to 11 of *this Handbook* must be complied with by **all *supervised persons***. The sector-specific sections (12 to 21) within *this Handbook* only provide additional *AML/CFT/CPF Codes of Practice* for particular business types in very limited circumstances.

1.5.2 Application of the *Money Laundering Order* to *supervised persons* carrying on business outside Jersey (overseas)

60. Article 10A of the *Money Laundering Order* explains and regulates the application of the *Money Laundering Order* to *supervised business* carried on outside Jersey.

61. Article 10A(2)(a) of the *Money Laundering Order* explains that a Jersey body corporate or other legal person registered in Jersey (*supervised person*) that carries on a *supervised business* through an overseas branch must comply with the *Money Laundering Order* in respect of that business, irrespective of whether it also carries on *supervised business* in or from within Jersey.

62. However, Article 10A(9) of the *Money Laundering Order* explains that a *supervised person* carrying on any of the business activities described in paragraphs 18 to 22 of Part 3 of Schedule 2 to the *Proceeds of Crime Law* need not comply with paragraphs (2), (3) and (4) in a country or territory outside Jersey in respect of their *supervised business*.

63. Notwithstanding the above paragraph, all the provisions of the *Money Laundering Order* apply to a *supervised person* that is a **legal person** carrying on *supervised business* anywhere in the world. However, in practice this may not apply to all *supervised persons* carrying on *supervised business* on the basis that some businesses currently registered under the *Supervisory Bodies Law* are either sole practitioners or Jersey customary law partnerships.

64. Article 10A(3) of the *Money Laundering Order* requires a *supervised person* (subject to Article 10A(9), see above) who: (i) is registered, incorporated or otherwise established under Jersey law, but who is not a legal person; and (ii) carries on a *supervised business* in or from within Jersey, to apply measures that are at least equivalent to the requirements of the *Money Laundering Order* in respect of any *supervised business* carried on by that person through an overseas branch. This requirement will apply to a limited partnerships registered under the Limited Partnerships (Jersey) Law 1994 and general partnership established under Jersey customary law.

> Note that the term "registered, incorporated or otherwise established" in Article 10A(5) of the *Money Laundering Order* is intended to be understood only to refer to the creation of a legal arrangement. In particular, it is not intended that "registered" be understood in the more general sense of registering under commercial or other legislation, or that "established" be understood in the more general sense of establishing a branch or representative office.

65. Article 10A(2)(b) of the *Money Laundering Order* requires a Jersey body corporate or other legal person (*supervised person*) registered in Jersey (subject to Article 10A(9) of the *Money Laundering Order*, see above) to ensure that any legal person that is majority owned or controlled by that person (referred to in the *Money Laundering Order* as a "subsidiary") applies measures that are at least equivalent to the requirements of the *Money Laundering Order* in respect of any *supervised business* carried on outside Jersey by that subsidiary.

66. Article 10A(4) of the *Money Laundering Order* requires a *supervised person* (subject to Article 10A(9) of the *Money Laundering Order,* see above) who: (i) is registered, incorporated or otherwise established under Jersey law, but who is not a legal person; and (ii) carries on a *supervised business* in or from within Jersey, to ensure that any subsidiary applies measures that are at least equivalent to the requirements of the *Money Laundering Order* in respect of any *supervised business* carried on outside Jersey by that subsidiary. This requirement will apply to a limited partnership registered under the Limited Partnerships (Jersey) Law 1994 and general partnership established under Jersey customary law.

67. In summary, Jersey companies and other legal persons registered in Jersey (subject to Article 10A(9) of the *Money Laundering Order,* see above) are covered by Article 10A(2) of the *Money Laundering Order* in relation to their overseas branches and subsidiaries. Other types of entity who do not have legal personality but who are constituted under Jersey law fall into Articles 10A(3) and (4) of the *Money Laundering Order* in relation to their overseas branches and subsidiaries.

68. Article 10A(6) of the *Money Laundering Order* requires a *supervised person* (subject to Article 10A(9) of the *Money Laundering Order,* see above) to take reasonable steps to comply with paragraphs (2), (3) and (4) to the extent that the law of the country or territory in which that person carries on a *supervised business*, or has a subsidiary carrying on such a business, does not have the effect of prohibiting or preventing the *supervised person* from taking such steps. If the *supervised person* does not comply with paragraphs (2), (3) and (4), the following steps must be taken by the *supervised person*: (i) the *JFSC* must be informed that this is the case; (ii) other reasonable steps to deal effectively with the risk of *money laundering* and the *financing of terrorism or proliferation financing* must be taken.

69. If a *supervised person* carries on a *supervised business* or has a subsidiary carrying on such a business overseas that has more stringent requirements than those set out in the *Money Laundering Order*, Article 10A(10) of the *Money Laundering Order* requires that the *supervised person* ensure that the more stringent requirements are complied with.

1.5.3 Application of *AML/CFT/CPF Codes of Practice* to *supervised persons* carrying on business outside Jersey (overseas)

70. By virtue of Articles 5, 6 and 22 of the *Supervisory Bodies Law*, a *supervised person* (subject to Article 10A(9) of the *Money Laundering Order,* see above) that is a company incorporated in Jersey that carries on a *supervised business* through an overseas branch must comply with the *AML/CFT/CPF Codes of Practice* in respect of that business, irrespective of whether it also carries on *supervised business* in or from within Jersey.

71. By concession, measures that are at least equivalent to *AML/CFT/CPF Codes of Practice* may be applied as an alternative to complying with the *AML/CFT/CPF Codes of Practice*.

72. A *supervised person* (subject to Article 10A(9) of the *Money Laundering Order,* see above) who (i) is registered, incorporated or otherwise established under Jersey law, but who is not a Jersey incorporated company; and (ii) carries on a *supervised business* in or from within Jersey, must apply measures that are at least equivalent to *AML/CFT/CPF Codes of Practice* in respect of any *supervised business* carried on by that person through an overseas branch. This requirement will apply to a foundation or partnership established under Jersey law.

> Note that the term "registered, incorporated or otherwise established" is intended to be understood only to refer to the creation of a legal person or legal arrangement.

73. A *supervised person* (subject to Article 10A(9) of the *Money Laundering Order,* see above) that is a Jersey incorporated company must ensure that any subsidiary applies measures that are at least equivalent to *AML/CFT/CPF Codes of Practice* in respect of any *supervised business* carried on outside Jersey by that subsidiary.

74. A *supervised person* (subject to Article 10A(9) of the *Money Laundering Order,* see above) who (i) is registered, incorporated or otherwise established under Jersey law, but who is not a Jersey incorporated company; and (ii) carries on a *supervised business* in or from within Jersey, must ensure that any subsidiary applies measures that are at least equivalent to *AML/CFT/CPF Codes of Practice* in respect of any *supervised business* carried on outside Jersey by that subsidiary. This requirement will apply to a foundation or partnership established under Jersey law.

75. Where overseas provisions prohibit compliance with one or more of the *AML/CFT/CPF Codes of Practice* (or measures that are at least equivalent), the requirements do not apply and the *JFSC* must be informed that this is the case. In such circumstances, the *AML/CFT/CPF Codes of Practice* require a *supervised person* to take other reasonable steps to effectively deal with the risk of *money laundering*, the *financing of terrorism*, and the *financing of proliferation*.

1.6 Definition of *supervised business*

76. *Supervised business* is defined in Article 1 of the *Supervisory Bodies Law*. This reflects the definition of *financial services business* as provided by Article 36 of the *Proceeds of Crime Law* (which in turn refers to Schedule 2 of the *Proceeds of Crime Law)*.

77. In practice, this means that all activities listed in Schedule 2 of the *Proceeds of Crime Law* are covered by the term *supervised business*.

78. Sector-specific sections for *supervised persons* subject to the funds, security issuers and their service providers, *TCSPs, Wire Transfers Regulations, prepaid cards, AMLSPs, VASPs, real estate agents, high value dealers, Lawyers and Accountants* are set out at Sections 12-21 of *this Handbook* and provide some additional *AML/CFT/CPF Codes of Practice* and *Guidance notes* for *supervised persons* carrying on those types of business.

1.7 *Business relationships* and *one-off transactions*

79. The terms *business relationship* and *one-off transaction* are defined in the Glossary of *this Handbook*.

Guidance notes

80. A *supervised person* may demonstrate that the basis upon which it has determined the value of a transaction for the purposes of Article 4 of the *Money Laundering Order* (e.g., to determine whether a transaction falls within the definition of a *one-off transaction* described in that Article) is appropriate where it applies the value of the underlying asset(s) to which the instruction relates. For example, regarding services provided in respect of a trust, a *supervised person* may apply the value of the trust assets.

81. Where a value to the underlying assets cannot be determined, or no value for the underlying assets is readily available or ascertainable, the *supervised person* should assume the value of the transaction to be €15,000 or more. Please note the lower thresholds for *MVTS*, *VASP* or operating a casino.

82. With reference to paragraph 81, persons carrying on *MVTS, VASP* or operating a casino should apply their specific transaction thresholds set out in Article 4 of the *Money Laundering Order*.

83. Further sector-specific guidance on determining the value of transactions is provided, where appropriate, in the relevant sector-specific sections.

84. Where a transaction is likely to become a *one-off transaction* or develop into a *business relationship*, the *supervised person* should consider undertaking *identification measures* at the outset.

85. Where the *supervised person* suspects *money laundering,* the *financing of terrorism or proliferation financing* whilst undertaking the above, they should refer to Section 9 of *this Handbook*.

1.8 Risk-based approach

Overview

86. To assist the overall objective of detecting and preventing *money laundering*, the *financing of terrorism*, and the *financing of proliferation*, *this Handbook* adopts a risk-based approach. Such an approach:

- recognises that the *money laundering*, *financing of terrorism*, and *financing of proliferation* threat to a *supervised person* varies across *customers*, countries and territories, products and delivery channels;
- allows a *supervised person* to differentiate between *customers* in a way that matches risk in a particular *supervised person*;
- while establishing minimum standards, allows a *supervised person* to apply its own approach to *systems and controls*, and arrangements in particular circumstances;
- helps to produce a more cost-effective system.

87. A risk-based approach requires steps to be taken to identify how a *supervised person* could be used for *money laundering*, the *financing of terrorism*, or the *financing of proliferation* and establishing the most effective and proportionate way to manage and mitigate the risks in the same way as for all business risks faced by a *supervised person*.

88. The possibility of being used to assist with *money laundering,* the *financing of terrorism*, and the *financing of proliferation* poses many risks for *supervised persons* including:

- criminal and disciplinary sanctions for the *supervised person* and for *key* and *principal persons;*
- civil action against the *supervised person* as a whole and against individual staff; and
- damage to reputation leading to loss of business.

89. *Systems and controls* will not detect and prevent all *money laundering*, *terrorist financing,* or *proliferation financing* activity. A risk-based approach will, however, serve to balance the cost burden placed on a *supervised person* and on its *customers* with a realistic assessment of the threat of it being used in connection with *money laundering,* the *financing of terrorism,* or the *financing of proliferation* by focusing effort where it is needed and has most impact.

90. How a risk-based approach is applied will also depend on the structure of the *supervised person's* business, its size and the nature of its products and services.

91. The *policies and procedures* put in place should be proportionate to the size of the business and the identified risks.

92. *Policies and procedures* may be more straightforward for smaller businesses. Such businesses may offer a smaller range of products or services, with most *customers* falling into similar categories. In these circumstances, a simpler approach may be appropriate for most *customers*, with the focus being on those *customers* that fall outside the usual categories. Larger businesses with a small range of products or services can put standard *AML/CFT/CPF policies and procedures* in place based on generic profiles of *customers*.

93. In more complex *business relationship*s, risk assessment, mitigation, and ongoing monitoring will be more sophisticated and will consider additional information held and knowledge of the *customer's* business activities.

94. An effective and documented risk-based approach will enable a *supervised person* to justify its position on managing *money laundering,* the *financing of terrorism*, *and* the *financing of proliferation* risks to law enforcement, the courts, regulators, and supervisory bodies.

1.9 Equivalence of requirements in other countries and territories

1.9.1 Equivalent business

95. Articles 16 and Part 3A of the *Money Laundering Order* respectively permit reliance to be placed on an *obliged person* and exemptions from *CDD* requirements to be applied to a *customer* carrying on a *supervised business* that is overseen for *AML/CFT/CPF* compliance in Jersey or carrying on business that is *equivalent business*. Sections dealing with the acquisition of a business or block of *customers* and verification of identity also provide concessions from *AML/CFT/CPF Codes of Practice* on a similar basis.

96. *Equivalent business* is defined in Article 5 of the *Money Laundering Order*.

97. The condition set out in Article 5 requiring that the business must be subject to requirements to combat *money laundering,* the *financing of terrorism,* and the *financing of proliferation* consistent with those in the *FATF Recommendations* will be satisfied, **among other things**, where a person is located in an equivalent country or territory.

1.9.2 Equivalent countries and territories

98. With effect from 31 May 2021, the *JFSC* no longer maintains a list of equivalent countries and territories within *this Handbook*. Guidance to assist *supervised persons* to determine equivalence is set out in Section 1.9.3 of *this Handbook*.

99. A country or territory may be considered to be equivalent where:

a. *Financial Institutions* and *DNFBPs* are required to take measures to detect and prevent *money laundering*, the *financing of terrorism*, and the *financing of proliferation* that are consistent with those in the *FATF Recommendations*.

b. *Financial Institutions* and *DNFBPs* are supervised for compliance with those requirements by a regulatory or supervisory authority.

1.9.3 Determining equivalence

100. Requirements for measures to be taken by an *obliged person* or *customer* will be considered to be consistent with the *FATF Recommendations* only where those requirements are established by law, regulation, or other enforceable means.

101. In determining whether or not the requirements for measures to be taken in a country or territory are consistent with the *FATF Recommendations*, a *supervised person* should have regard for the following:

› generally - whether or not the country or territory is a member of the *FATF*, a member of a FSRB or subject to its assessment and follow-up process, a member state of the *EU*, or a member of the *EEA;*

› specifically - whether a country or territory is compliant or largely compliant with those *FATF Recommendations* that are directly relevant to the application of available concessions. These are *FATF Recommendations* 10-13, 15-21 and 26. Where a person with a specific connection to a *customer* is a *DNFBP* (a term that is defined by the *FATF*), then *FATF Recommendations* 22, 23 and 28 will be relevant;

- specifically – the extent to which a country or territory is achieving *FATF's* immediate outcomes that are directly relevant to the application of available concessions, namely whether *FATF* immediate outcomes 3 and 4 are assessed at a high or substantial level of effectiveness;
- the following sources may be used to determine whether a country or territory is compliant or largely compliant or achieving the Immediate Outcomes:
    a. the laws and instruments that set requirements in place in that country or territory;
    b. recent independent assessments of that country's or territory's framework to combat *money laundering*, the *financing of terrorism*, and the *financing of proliferation*, such as those conducted by the *FATF, FSRBs*, the *IMF* and the World Bank (and published remediation plans);
    c. other publicly available information concerning the effectiveness of a country's or territory's framework.

102. Where a *supervised person* assesses whether a country or territory is an equivalent country or territory, the *supervised person* must conduct an assessment process comparable to that described above and must be able to demonstrate on request the process undertaken and the basis for its conclusion.

103. Links to potential sources of additional information are included in **Appendix B** of *this Handbook*. These are not intended to be exhaustive, nor are they placed in any order of priority. Independent research and judgement will be expected to cater for the requirements in the individual case.

2 CORPORATE GOVERNANCE

2.1 Overview of section

1. Corporate governance is the system by which enterprises are directed and controlled and their risks managed. For *supervised persons*, *money laundering*, the *financing of terrorism*, and the *financing of proliferation* are risks that must be managed in the same way as other business risks.

2. Under the general heading of corporate governance, this section considers:

- board responsibilities for the prevention and detection of *money laundering, the countering of terrorist financing,* and the *countering of proliferation financing;*
- requirements for systems and controls, training, and awareness;
- the appointment of a ***MLCO*** and ***MLRO***.

3. *This Handbook* describes a *supervised person*'s general framework to combat *money laundering*, the *financing of terrorism*, and the *financing of proliferation* as its systems and controls. *This Handbook* refers to the way in which those *systems and controls* are implemented into the day-to-day operation of a *supervised person* as its *policies and procedures*.

4. Where a *supervised person* is not a company but is, for example, a partnership, references in this section to "the board" should be read as meaning the senior management of that person, including the board of a legal arrangement's *Governing body*. In the case of a *sole trader*, "the board" will be the *sole trader*. In the case of an overseas company carrying on a *supervised business* in Jersey through a branch, "the board" should be read as including the local management function of that branch in Jersey.

5. Section 15 of *this Handbook* details how a *supervised person* who meets certain criteria to appoint an *AMLSP* may fulfil its obligations.

2.2 *AML/CFT/CPF measures*

Statutory requirements (paraphrased wording)

6. *In accordance with Article 37 of the Proceeds of Crime Law, a relevant person must take prescribed measures to prevent and detect money laundering and the financing of terrorism. Failure to take such measures is a criminal offence and, where such an offence is proved to have been committed with the consent or connivance of, or to be attributable to neglect on the part of, a director or manager or officer of the relevant person, they too shall be deemed to have committed a criminal offence.*

7. *Article 37 enables the Minister for External Relations and Financial Services to prescribe by Order the measures that must be taken (including measures not to be taken):*

i) by a relevant person; and

ii) by an AMLSP appointed by a relevant person.

These measures are established in the Money Laundering Order.

2.3 Board responsibilities

Overview

8. The key responsibilities of the board, set out in further detail below, are to:

- identify the *supervised person*'s *money laundering*, the *financing of terrorism*, and the *financing of proliferation* risks;
- ensure that its *systems and controls* are appropriately designed and implemented to manage those risks; and
- ensure that sufficient resources are devoted to fulfilling these responsibilities.

9. The board is assisted in fulfilling these responsibilities by a *MLCO* and *MLRO*. Larger or more complex *supervised person*s may also require dedicated risk and internal audit functions to assist in the assessment and management of *money laundering*, the *financing of terrorism*, and the *financing of proliferation* risk.

Statutory requirements (paraphrased wording)

10. *Article 11(1) of the Money Laundering Order requires a relevant person to establish and maintain appropriate and consistent policies and procedures in respect of the person's financial services business, and financial services business carried on by a subsidiary, to prevent and detect money laundering and the financing of terrorism.*

11. *Article 11(11) of the Money Laundering Order requires a relevant person to establish and maintain adequate procedures for monitoring compliance with and testing the effectiveness of: (i) its policies and procedures; (ii) its measures to promote AML/CFT/CPF awareness; and (iii) its training of relevant employees (see Section 10 of this Handbook).*

12. *Articles 7 and 8 of the Money Laundering Order require that a relevant person appoints a MLCO and a MLRO.*

AML/CFT/CPF Codes of Practice

[COP1] The board must conduct and record a *BRA* in respect of the *supervised person*. In particular, the board must consider, on an ongoing basis, the *supervised person's* risk appetite and the extent of the *supervised person's* exposure to *money laundering*, the *financing of terrorism*, and the *financing of proliferation* risks "in the round" or as a whole by reference to the *supervised person's* organisational structure, *customers*, the countries and territories with which those *customers* are connected, the products and services the *supervised person* provides and how those products and services are delivered. The assessment must consider the cumulative effect of risks identified, which may exceed the sum of each individual risk element. The board's assessment must be kept up to date (see section 2.3.1 of *this Handbook*).

[COP2] Based on its *BRA*, the board must establish a formal strategy to counter *money laundering*, the *financing of terrorism*, and the *financing of proliferation*. Where a *supervised person* forms part of a group operating outside the Island, that strategy may protect both its global reputation and its Jersey business.

[COP3] Considering the conclusions of the *BRA* and strategy, the board must:

- organise and control its affairs in a way that effectively mitigates the risks that it has identified, including areas that are complex; and
- be able to demonstrate the existence of adequate and effective *systems and controls* (including *policies and procedures*) to counter *money laundering*, the *financing of terrorism*, and the *financing of proliferation* (see Section 2.4 of *this Handbook*).

[COP4] The board must document its *systems and controls* (including *policies and procedures*) and clearly apportion responsibilities for countering *money laundering*, the *financing of terrorism*, or the *financing of proliferation*, and, in particular, responsibilities of the *MLCO* and *MLRO* (see sections 2.6 and 2.7 of *this Handbook*).

[COP5] The board must assess both the effectiveness of, and compliance with, *systems and controls* (including *policies and procedures*) and take prompt action necessary to address any deficiencies (see sections 2.4.1 and 2.4.2 of *this Handbook*).

[COP6] The board must consider what barriers (including cultural barriers) exist to prevent the operation of effective *systems and controls* (including *policies and procedures*) to counter *money laundering*, the *financing of terrorism*, or the *financing of proliferation*, and must take effective measures to address them (see section 2.4.3 of *this Handbook*).

[COP7] The board must notify the *JFSC* immediately in writing of any material failures to comply with the requirements of the *Money Laundering Order* or the *AML/CFT/CPF Handbook*.

2.3.1 BRA

AML/CFT/CPF Codes of Practice

[COP8] A *supervised person* must maintain appropriate *policies and procedures* to enable it, when requested by the *JFSC*, to make available to that authority a copy of its *BRA*.

Guidance notes

13. When considering a risk appetite for the *supervised person's* business, the board may wish to examine the following factors (note the below list is not exhaustive):

- are they prepared to accept only a certain proportion of business rated at each risk level? For example, the board may only have an appetite for high-risk *customer*s to form a set proportion of their overall fee income or assets under management;
- are there any country connections or *customer* risk levels with which the board are not prepared to engage?
- are there any *sensitive activities* or industries undertaken by potential *customer*s, which the board are not prepared to take on?
- will the board accept *business relationships* or *one-off transactions* where *PEPs* are involved?
- how do the characteristics of the *supervised person* (e.g., business sector, type of products and services offered) potentially expose it to greater *ML, TF,* and/or *PF* risk?
- what types of *customer*s and activity are considered to be outside of Jersey's national risk appetite? See Financial crime strategy, appetite and national risk assessments (gov.je)

14. It is important for the risk appetite to be sufficiently clear so that the board can articulate it when considering whether to establish a *business relationship* or carry out a *one-off transaction* with a *customer*. For example, it should not be so vague that it can be used to justify the acceptance of any business, no matter the risk level.

15. Equally, a clear risk appetite should not be wilfully ignored. For example, a high-risk potential *customer* offers an attractive fee proposition, so the business is accepted even though doing so would mean the *supervised person* exceeds the risk appetite's stated maximum proportion of high-risk business.

16. It is the responsibility of the board to ensure that *business relationships* and *one-off transactions* are maintained in accordance with the agreed risk appetite.

17. A *supervised person* may extend its existing risk management systems to address *money laundering/terrorist financing/proliferation financing* risks. The detail and sophistication of these systems will depend on the *supervised person's* size and the complexity of the business it undertakes. Ways of incorporating a *supervised person's BRA* will be governed by the size of the *supervised person* and how regularly compliance staff and the board are involved in day-to-day activities.

18. The board of a *supervised person* may demonstrate that it has considered its exposure to *money laundering*, the *financing of terrorism*, and the *financing of proliferation* risk by:

› involving all members of the board in determining the risks posed by *money laundering*, the *financing of terrorism,* and the *financing of proliferation* within those areas for which they have responsibility;

› considering organisational factors that may increase the level of exposure to the risk of *money laundering*, the *financing of terrorism,* and the *financing of proliferation*, e.g., outsourced aspects of regulated activities or compliance functions;

› considering the nature, scale and complexity of its business, the diversity of its operations (including geographical diversity), the volume and size of its transactions, and the degree of risk associated with each area of its operation;

› considering who its *customers* are and what they do, e.g., do its *customer*s engage in higher-risk activities (having regard for the *JFSC's* Sound Business Policy);

› considering whether any additional risks are posed by the countries, territories and areas with which its *customer*s are connected. Factors such as high levels of organised crime, increased vulnerabilities to corruption and inadequate frameworks to prevent and detect *money laundering, the financing of terrorism,* and the *financing of proliferation* will impact the risk posed by relationships connected with such countries, territories and areas;

› considering the characteristics of the products and services that it offers and assessing the associated vulnerabilities posed by each product and service. For example:

   a. products that allow a *customer* to "pool" third party funds will tend to be more vulnerable - because of the anonymity provided by the co-mingling of assets or funds belonging to several third parties by the *customer;*

   b. products such as standard current accounts are more vulnerable because they allow payments to be made to and from external parties, including cash transactions;

   c. conversely, those products that do not permit external party transfers or where redemption is permitted only to an account from which the investment is funded will be less vulnerable;

   d. products and services which make use of new and developing technologies, such as virtual assets, may pose a risk due to the increased anonymity which can be afforded by the asset to their users. There may also be a lack of experience in providing these new products, meaning the control environment may not be as effective.

› considering the risk that is involved in placing reliance on *obliged persons* to apply *reliance identification measures;*

- considering how it establishes and delivers products and services to its *customers*. For example, risks are likely to be greater where relationships may be established remotely (non-face-to-face), or may be controlled remotely by the *customer* (straight-through processing of transactions);
  - a *supervised person* may employ new and developing technologies to establish *business relationship*s with their *customers*, for example through a *Digital ID* application. As discussed further in Section 4.2.6 of *this Handbook*, the risks of using such technology to obtain evidence of identity should be considered, noting the particular characteristics of each application. This should be recorded in the *BRA*;
- considering the accumulation of risk for more complex *customers*.

19. When conducting a *BRA* care should be taken not to focus too much on any single factor. All factors (including those identified by a National Risk Assessment or similar), as well as the wider picture (and cumulative risk) should be considered.

20. Care should also be taken not to rely on a 'template' *BRA*, i.e., one previously prepared within the business or supplied by an external provider. The assessment should be customised to fully reflect and consider the unique types of *customer*s serviced by the business, the geographical areas to which it has exposure, and the specific products and services provided by the business.

21. With reference to new and developing technologies, the board should have a due diligence process in place to analyse and understand their risks, then apply a framework for how they will be monitored and managed going forward.

22. A generic example of how risk might be calculated in a *BRA* is set out below. Please note this methodology is for illustrational purposes only. It should not be construed as the *JFSC* taking a position on how risk should be calculated and represented in a *BRA*. Each *BRA* should uniquely consider and represent the risks and controls identified by the *supervised person*:

Impact (implications of event)	**Likelihood (of event happening)**	**Inherent Risk (impact x likelihood)**	**Impact and likelihood after controls applied**	**Residual risk (impact x likelihood after controls applied)**
3 – Significant impact on business.	3 – Very likely.	9 – High inherent risk.	Each rating may range from 1-3.	Possible scores: 1-9.
2 – Moderate impact on business.	2 – Moderately likely.	4 – Moderate inherent risk.	Each rating may range from 1-3.	Possible scores: 1-9.
1 – Minimal impact on business.	1 – Unlikely to happen.	1 – Low inherent risk.	Each rating may range from 1-3.	Possible scores: 1-9.

23. A generic example of a *BRA* is set out below. Please note the descriptions and scores assigned to these risks are for illustrational purposes only. They should not be construed as the *JFSC* taking a position on how these risks should be scored and/or controlled. Each *BRA* should uniquely consider and represent the risks and controls identified by the *supervised person*:

Risk descriptor	Impact	Likelihood	Inherent Risk	Controls applied	Residual Risk
Customer is involved in evasion of sanctions relating to *financing of proliferation.*	3 (Reputational damage, potential legal/regulatory sanctions).	2	6	Business will not engage with *customers* involved in shipping or have connections to Iran or *DPRK*. Reduces likelihood to 1.	3 x 1 = 3
Pandemic requiring national lockdown.	3 (Business unable to operate).	1	3	All staff able to work remotely. All *customer* transactions can be undertaken electronically. Reduces impact to 1.	1 x 1 = 1
Breach of *Money Laundering Order.*	3 (Reputational damage, potential legal/regulatory sanctions).	2	6	Staff receive training at on-boarding, and regularly thereafter. Staff are required to comply with *policies and procedures.* Breaches are recorded and considered at board meetings. Consideration includes trends analysis, lessons learned, training needs and strengthening controls. Reduces likelihood to 1.	3 x 1 = 3

24. In developing a risk-based approach, *supervised persons* need to ensure that the *BRA* can be understood by the board, other *relevant employees* and relevant third parties, e.g., auditors and the *JFSC*.

25. In the case of a *supervised person* that is dynamic and growing, the board may demonstrate that its *BRA* is kept up to date where it is reviewed annually. In some other cases, this may be too often, e.g., a *supervised person* with a stable *customer* base, products, and services. In all cases, the board may demonstrate that its *BRA* is kept up to date where it is reviewed when events (internal and external) occur that may materially change *money laundering, terrorist financing, and proliferation financing* risk.

26. It may be beneficial for *money laundering, financing of terrorism, and financing of proliferation* risks and controls to each be considered separately.

27. When reviewing a *BRA,* the board should ensure it captures all relevant risks and considers how effective the business' control environment is at managing those risks. Effectiveness can be evidenced by considering the findings of control testing such as periodic reviews and reviewing data collected by the *supervised person*.

28. Where gaps or deficiencies are identified during a *BRA* review, an action plan should be drawn up so they can be addressed. The action plan should form an integral part of the *BRA.*

29. Where a *supervised person* is subject to a regulatory Code of Practice (such as the Trust Company Business Code of Practice) there is also an obligation for a wider, operational *BRA* to be conducted. When preparing an *AML/CFT/CPF BRA* or *CRA*, factors in this operational *BRA* may be relevant. Therefore, a combined *AML/CFT/CPF* and operational *BRA* may be appropriate.

30. Risks that are not normally considered to be specific *money laundering/terrorist financing/proliferation financing* risks may also be relevant to an *AML/CFT/CPF BRA*, for example, credit risk, tax risk, investor eligibility risk, cyber security related risk etc.

31. It is likely that the *BRA* will be conducted by the *supervised person* prior to any *CRA*. When *a CRA* is prepared, the *BRA* may need to be updated (for example, to consider new risk factors, or the *supervised person's* changing risk tolerance/appetite).

32. For *supervised persons* who are operating as an agent of another *supervised person* (or have agents operating on their behalf), either the *supervised person* or the agent should determine, relative to the nature of their relationship, how each risk is to be identified, managed, and documented. This is particularly important in the case of *MVTS supervised persons*, whereby each agent may have bespoke risks which will need to be carefully identified, assessed, and managed.

2.4 Adequate and effective *systems and controls*

Overview

33. For *systems and controls* (including *policies and procedures*) to be adequate and effective in preventing and detecting *money laundering*, the *financing of terrorism*, the *financing of proliferation*, they will need to be appropriate to the circumstances of the *supervised person*. See Section 15 of *this Handbook* where an *AMLSP* appointed by a *supervised person* may provide *AMLSP services* relating to *systems and controls*.

Statutory requirements (paraphrased wording)

34. *Article 11(1) of the Money Laundering Order requires a relevant person to establish and maintain appropriate and consistent policies and procedures in respect of the person's financial services business, and financial services business carried on by a subsidiary, to prevent and detect money laundering, the financing of terrorism.*

35. *Parts 3, 3A, 4 and 5 of the Money Laundering Order set out the measures that are to be applied in respect of CDD, record-keeping and reporting.*

36. *Article 11(2) of the Money Laundering Order requires that policies and procedures established and maintained under Article 11(1) are appropriate and consistent having regard to the degree of risk of money laundering and the financing of terrorism taking into account: (i) the level of risk identified in a national or sector-specific risk assessment in relation to money laundering carried out in respect of Jersey; and (ii) the type of customers, business relationships, products and transactions with which the relevant person's business is concerned.*

37. *Article 11(3) lists several policies and procedures that must be established and maintained.*

38. *Article 11(9) of the Money Laundering Order requires a relevant person to take appropriate measures for the purpose of making employees whose duties relate to the provision of financial services ("relevant employees") aware of policies and procedures under Article 11(1) and of legislation in Jersey to counter money laundering and the financing of terrorism. Article 11(10) of the Money Laundering Order requires a relevant person to provide relevant employees with training in the recognition and handling of transactions carried out by or on behalf of persons who are, or appear to be, engaged in money laundering or the financing of terrorism.*

39. *Article 11(11) of the Money Laundering Order requires a relevant person to establish and maintain policies and procedures for monitoring compliance with and testing the effectiveness of: (i) its policies and procedures; (ii) its measures to promote AML/CFT awareness; and (iii) its training of relevant employees (see Section 10 of this Handbook).*

40. *When considering the type and extent of testing to be carried out under Articles 11(11) and 11(12) of the Money Laundering Order requires a relevant person to have regard to the risk of money laundering or financing of terrorism that exists in respect of the relevant person's business, and matters that have an impact on that risk, such as the size and structure of the relevant person.*

41. *Article 11(8) requires that a relevant person operating through branches or subsidiaries, which carry on financial services business, must communicate its policies and procedures, maintained in accordance with Article 11(1) of the Money Laundering Order, to those branches or subsidiaries. In addition, Article 11A of the Money Laundering Order requires group programmes for information sharing (see Section 2.8 of this Handbook).*

AML/CFT/CPF Codes of Practice

[COP9] A *supervised person* must establish and maintain appropriate and consistent *systems and controls* to prevent and detect *money laundering*, the *financing of terrorism*, and the *financing of proliferation*, that enable it to:

- apply the *policies and procedures* referred to in Article 11 of the *Money Laundering Order*;
- apply *CDD* measures – in line with Sections 3 to 8 of *this Handbook*;
- report to the *FIU* when it knows, suspects, or has reasonable grounds to know or suspect that another person is involved in *money laundering* or the *financing of terrorism*, including attempted transactions – in line with Section 9 of *this Handbook*;
- adequately screen *relevant employees* when they are initially employed, make *employees* aware of certain matters and provide training – in line with Section 10 of *this Handbook*;
- keep complete records that may be accessed on a timely basis – in line with Section 11 of *this Handbook*;
- liaise closely with the *JFSC* and the *FIU* on matters concerning vigilance, *systems, and controls* (including *policies and procedures*);

- communicate *policies and procedures* to overseas branches and subsidiaries (subject to Article 10A(9) of the *Money Laundering Order* (see section 1.4.2 of *this Handbook*), and monitor compliance therewith; and
- monitor and review instances where exemptions are granted to *policies and procedures*, or where *controls* are overridden.

[COP10] In addition to those listed in Article 11(3) of the *Money Laundering Order*, a *supervised person* must have *policies and procedures* for:

- *customer* acceptance (and rejection), including approval levels for higher risk *customers*;
- the use of transaction limits and management approval for higher risk *customers*;
- placing reliance on *obliged persons*;
- applying exemptions from *CDD* requirements under Part 3A of the *Money Laundering Order* and *enhanced CDD* measures under Articles 15, and 15A of the *Money Laundering Order*;
- keeping documents, data or information obtained under *identification measures* up-to-date and relevant changes in beneficial ownership and/or control, including beneficiaries under a life insurance policy;
- taking action in response to notices highlighting countries and territories in relation to which the *FATF* has called for the application of countermeasures or *enhanced CDD measures*;
- taking action to comply with the Targeted Financial Sanctions Measures and the Directions Law.

[COP11] A *supervised person* must check that the *systems and controls* (including *policies and procedures*) are operating effectively and test that they are complied with.

2.4.1 Effectiveness of systems and controls

Guidance notes

42. A *supervised person* may demonstrate that it checks that *systems and controls* (including *policies and procedures*) are adequate and operating effectively where the Board periodically considers the efficacy (capacity to have the desired outcome) of those *systems and controls* (including *policies and procedures*, and those in place at branches and in respect of subsidiaries) considering:

- changes to its business activities or *BRA*;
- information published from time to time by the *JFSC* or *FIU*, e.g., findings of supervisory and themed examinations and typologies;
- changes made or proposed in respect of new legislation, *AML/CFT/CPF Codes of Practice* issued under the *Supervisory Bodies Law* or *Guidance*;
- resources available to comply with the *Anti-Money Laundering and Counter-Terrorism Legislation* and *AML/CFT/CPF Codes of Practice* issued under the *Supervisory Bodies Law*, in particular resources provided to the *MLCO* and *MLRO*, to apply *enhanced CDD measures* and to scrutinise transactions.

43. A *supervised person* may demonstrate that it checks that *systems and controls* (including *policies and procedures*) are operating effectively where the board periodically considers the effect of those *systems and controls* (including *policies and procedures*, and those in place at branches and in respect of subsidiaries) considering the information that is available to it, including:

- reports presented by the *MLCO* and others (e.g., where appropriate, risk management and internal audit functions) on compliance matters and *MLRO* on reporting;
- reports summarising findings from supervisory and themed examinations and action taken or being taken to address recommendations;
- the number and percentage of *customers* that have been assessed by the *supervised person* as presenting a higher risk;
- the number of applications to establish *business relationships* or carry-out *one-off transactions* which have been declined due to *CDD* issues, along with reasons;
- the number of *business relationships* terminated due to *CDD* issues, along with reasons;
- the number of "existing *customers*" that have still to be remediated under Section 4.9.2 *of this Handbook*;
- details of failures by an *obliged person* or *customer* to provide information and evidence on demand and without delay under Articles 16, 16A and 17B-D of the *Money Laundering Order*, and action taken;
- the number of alerts generated by automated ongoing monitoring systems;
- the number of internal *SARs* made to the *MLRO* (or *Deputy MLRO*), the number of subsequent external *SARs* submitted to the *FIU*, and timeliness of reporting (by business area if appropriate);
- inquiries made by the *FIU*, or production orders received, without issues having previously been identified by *CDD* or reporting *policies and procedures*, along with reasons;
- results of testing of awareness of *relevant employees* with *policies and procedures* and legislation;
- the number and scope of exemptions granted to *policies and procedures*, including at branches and subsidiaries, along with reasons.

44. The level of systems and controls, and the extent to which monitoring needs to take place will be affected by:

- the *supervised person*'s size;
- the nature, scale and complexity of its operations;
- the number of different business types it is involved in;
- the types of services it offers and how it delivers those services;
- the type of business transactions it becomes involved in or advises on;
- its overall risk profile.

45. Areas which are required under the *Money Laundering Order* to be covered in *systems and controls* include (but are not limited to):

- the manner in which disclosures are to be made to the *MLRO*;
- the circumstances in which delayed *CDD* is permitted;

- when outsourcing of *CDD* obligations or reliance on third parties will be permitted, and on what conditions;
- *CDD* requirements to be met for simplified, standard and *enhanced due diligence*;
- how the *supervised person* will restrict work being conducted for a *customer* where *CDD* has not been completed.

46. Issues which may also be covered in *systems and controls* include:

- the level of personnel permitted to exercise discretion on the risk-based application of the *Money Laundering Order* and *this Handbook*, and under what circumstances;
- when cash payments will be accepted;
- when payments will be accepted from or made to third parties;

the *supervised person's* policy for applying *LPP*. Note that *LPP* is only applicable to *Lawyers* – see Section 20.5.1 of *this Handbook*.

47. For *supervised persons* with an agent relationship with another natural or legal person, it is the responsibility of the *supervised person* to ensure that they have sufficient oversight or understanding of the operations of the agent to be able to demonstrate adequate *systems and controls* in relation to this relationship.

2.4.2 Testing of compliance with *systems and controls*

Guidance notes

48. A *supervised person* may demonstrate that it has tested compliance with *systems and controls* (including *policies and procedures*) where the board periodically considers the means by which compliance with its *systems and controls* (including *policies and procedures*) has been monitored, compliance deficiencies identified, and details of action taken or proposed to address any such deficiencies.

49. A *supervised person* may demonstrate that it has tested compliance with *systems and controls* (including *policies and procedures*) where testing covers all the *policies and procedures* maintained in line with Article 11(1) of the *Money Laundering Order* and the *AML/CFT/CPF Codes of Practice*, in particular:

- the application of simplified and *enhanced CDD measures*;
- reliance placed on *obliged persons* under Article 16 of the *Money Laundering Order*;
- action taken in response to notices highlighting countries and territories in relation to which the *FATF* has called for the application of countermeasures or *enhanced CDD measures*;
- action taken to comply with the *Targeted Financial Sanctions Measures* and the *Directions Law*; and
- the number or type of *employees* who have received training, the methods of training and the nature of any significant issues arising from the training.

2.4.3 Consideration of cultural barriers

Overview

50. The implementation of *systems and controls* (including *policies and procedures*) for the prevention and detection of *money laundering*, the countering of *terrorist financing*, and the countering of *proliferation financing* does not remove the need for a *supervised person* to address cultural barriers that can prevent effective control. Human factors, such as the inter-relationships between different *employees*, and between *employees* and *customers*, can result in the creation of damaging barriers.

51. Unlike *systems and controls* (including *policies and procedures*), the prevailing culture of an organisation is intangible. As a result, its impact on a *supervised person* can sometimes be difficult to measure.

Guidance notes

52. A *supervised person* may demonstrate that it has considered whether cultural barriers might hinder the effective operation of *systems and controls* (including *policies and procedures*) to prevent and detect *money laundering*, counter *terrorist financing*, and counter *proliferation financing* where the board considers the prevalence of the following factors:

- an unwillingness on the part of employees to subject high value (and therefore important) *customers* to effective *CDD* measures for commercial reasons;
- pressure applied by management or *customer* relationship managers outside Jersey upon employees in Jersey to transact without first conducting all relevant *CDD*;
- undue influence exerted by relatively large *customers* in order to circumvent *CDD measures*;
- excessive pressure applied on employees to meet aggressive revenue-based targets, or where *employee* or management remuneration or bonus schemes are exclusively linked to revenue-based targets;
- an excessive desire on the part of *employees* to provide a confidential and efficient *customer* service;
- design of the *customer* risk classification system in a way that avoids rating any *customer* as presenting a higher risk;
- the inability of employees to understand the commercial rationale for *business relationships*, resulting in a failure to identify non-commercial and therefore potential *money laundering, terrorist financing,* or *proliferation financing* activity;
- negative handling by managerial staff of queries raised by more junior *employees* regarding unusual, complex or higher risk activity and transactions;
- an assumption on the part of more junior employees that their concerns or suspicions are of no consequence;
- a tendency for line managers to discourage *employees* from raising concerns due to lack of time and/or resources, preventing any such concerns from being addressed satisfactorily;
- dismissal of information concerning allegations of criminal activities on the grounds that the *customer* has not been successfully prosecuted or lack of public information to verify the veracity of allegations;
- the familiarity of *employees* with certain *customers* resulting in unusual or higher risk activity and transactions within such relationships not being identified as such;
- little weight or significance is attributed to the role of the *MLCO* or *MLRO*, and little cooperation between these post-holders and *customer*-facing *employees*;

- actual practices applied by *employee*s do not align with *policies and procedures*;
- *employee* feedback on problems encountered applying *policies and procedures* is ignored;
- non-attendance of senior *employees* at training sessions, e.g. based on a mistaken belief that they cannot learn anything new or because they have too many other competing demands on their time.

2.4.4 Outsourcing

Overview

53. In a case where a *supervised person* outsources a particular activity, it bears the ultimate responsibility for the duties undertaken in its name. This will include the requirement to determine that the external party has in place satisfactory *systems and controls* (including *policies and procedures*), and that those *systems and controls* (including *policies and procedures*) are kept up to date to reflect changes in requirements. See the table below for details of which *CDD* activities may be outsourced.

<table>
<tr><th>CDD (always the ultimate responsibility of the supervised person)</th><th colspan="2">Activities which may be outsourced</th></tr>
<tr><td rowspan="7">Identification measures</td><td colspan="2">Risk assessment.</td></tr>
<tr><td colspan="2">Identification of customer.</td></tr>
<tr><td colspan="2">Identification of third parties.</td></tr>
<tr><td>Identification of person acting for customer.</td><td>Verify authority to act.</td></tr>
<tr><td rowspan="2">Where customer is not an individual:</td><td>Understand ownership/control structure.</td></tr>
<tr><td>Identification of Beneficial owner and/or controllers.</td></tr>
<tr><td colspan="2">Obtain information on purpose/nature.</td></tr>
<tr><td rowspan="2">Ongoing monitoring</td><td colspan="2">Scrutinising transactions/activity.</td></tr>
<tr><td colspan="2">Keep documents/information up to date.</td></tr>
</table>

54. Depending on the nature and size of a *supervised person*, the roles of the *MLCO* and *MLRO* may require additional support and resourcing. Where a *supervised person* elects to bring in additional support, or to delegate areas of the *MLCO* or *MLRO* functions to external parties, the *MLCO* or *MLRO* will remain directly responsible for their respective role, and the board will remain responsible for overall compliance with the *Anti-Money Laundering and Counter-Terrorism Legislation* (and by extension, also *this Handbook*). Note that the *AML/CFT/CPF Codes of Practice* at paragraphs 90 and 103 below provide that the role of the *MLCO* and *MLRO* must be undertaken by an employee of the *supervised person* based in Jersey, unless the specific circumstances set out in the sub-paragraphs to those specific *Codes of Practice* apply.

55. The *JFSC* has also issued an Outsourcing policy or *supervised persons*, which outlines its own set of requirements and obligations in respect of outsourcing.

56. Where an *AMLSP* performs *AMLSP services* on behalf of an *AMLSP Direct Customer* and such *AMLSP services* are consistent with the *Money Laundering Order* and the standards set out in the *AML/CFT/CPF Codes of Practice* and *Guidance notes* for *AMLSPs* in *this Handbook*, the performance of such *AMLSP services* **is not** subject to the Outsourcing policy but **is** subject to Section 15 of *this Handbook*.

AML/CFT/CPF Codes of Practice

[COP12] All *supervised persons* must comply with the *JFSC*'s Outsourcing policy, except where an *AMLSP* performs *AMLSP services* on behalf of an *AMLSP Direct Customer* and such *AMLSP services* are consistent with the *Money Laundering Order* and the standards set out in the *AML/CFT/CPF Codes of Practice* and *Guidance notes* for *AMLSPs* in *this Handbook*.

[COP13] A *supervised person* must consider the effect that outsourcing has on *money laundering*, *terrorist financing*, and *proliferation financing* risk, in particular where an *MLCO* or *MLRO* is provided with additional support from other parties, either from within group or externally.

[COP14] A *supervised person* must assess possible *money laundering*, *terrorist financing*, and *proliferation financing* risk associated with outsourced functions, record its assessment, and monitor any risk on an ongoing basis.

[COP15] Where an outsourced activity is a *supervised business activity*, then a *supervised person* must be satisfied that the provider of the outsourced services has in place *policies and procedures* that are consistent with those required under the *Money Laundering Order* and, by association, *this Handbook*.

[COP16] A *supervised person* must be satisfied that knowledge, suspicion, or reasonable grounds for knowledge or suspicion of *money laundering*, the *financing of terrorism* or *proliferation financing* activity will be reported by the provider of the outsourced service to the *MLRO* (or *Deputy MLRO*) of the *supervised person*.

2.5 Risk Questionnaires

Overview

57. Since 2018, the *JFSC* has collected data from *supervised persons* on an annual basis to support our implementation of a risk-based approach to supervision. This includes:

› organisational/footprint data;

› *AML/CFT/CPF* compliance data; and

› data regarding a *supervised person's customers*.

58. This data is used to:

› improve our understanding of the activities undertaken by *supervised persons* and modify our risk-based approach; accordingly, and

› assist in the preparation of national risk assessments for Jersey.

59. To collect the above-referenced data, the *JFSC* will issue one or more *Risk Questionnaires* to *supervised person*s. The content of a *Risk Questionnaire* will differ based on the business sector of the *supervised person*. At the discretion of the *JFSC*, some sectors or parts thereof may not be included in a particular *Risk Questionnaire* exercise.

60. A set period will be provided, by the end of which all *supervised person*s receiving a *Risk Questionnaire* are required to complete and return it to the *JFSC*.

AML/CFT Codes of Practice

[COP17] When in receipt of a *Risk Questionnaire* from the *JFSC*, a *supervised person* must complete and return it by the deadline provided.

Guidance notes

61. To prepare for a *Risk Questionnaire*, a *supervised person* may consider reviewing relevant *Guidance notes* issued by the *JFSC* in previous data collection exercises. The *supervised person* can then update its *systems and controls* (including *policies and procedures*), so the required data is collected during the usual course of business.

62. For each data collection exercise, the *JFSC* will provide specific guidance on how to complete the *Risk Questionnaire*. This includes guidance for the organisational/footprint part of the *Risk Questionnaire* and the sector-specific parts. A *supervised person* should read the relevant guidance in full before completing a *Risk Questionnaire*.

63. A *supervised person* should consider storing the required data in a format which can be easily reviewed, extracted, and transferred to a *Risk Questionnaire*. It may also be appropriate to ensure any supporting documentation which was used in completing a *Risk Questionnaire* can be easily accessed, if required.

64. Where a *supervised person* is unable to meet the deadline provided due to extenuating circumstances, a request should be made to that *supervised persons'* supervisor as early as possible, seeking an extension.

2.6 The *MLCO*

Overview

65. The *Money Laundering Order* requires a *supervised person* or the *supervised persons' AMLSP*, where applicable (see section 15 of *this Handbook*), to appoint an individual as *MLCO*, and tasks that individual with the function of monitoring its compliance with legislation in Jersey relating to *money laundering*, the *financing of terrorism*, and the *financing of proliferation* and *AML/CFT/CPF Codes of Practice* issued under the *Supervisory Bodies Law*. The objective of this requirement is to require *supervised persons* to clearly demonstrate how they ensure compliance with the requirements of the same.

66. The *Money Laundering Order* also requires a *supervised person* to maintain adequate procedures for:

a. monitoring compliance with, and testing the effectiveness of, *policies and procedures*; and

b. monitoring and testing the effectiveness of measures to raise awareness and training. When considering the type and extent of compliance testing to be carried out, a *supervised person* shall have regard to the risk of *money laundering*, the *financing of terrorism*, and the *financing of proliferation* and matters that have an impact on risk, such as size and structure of the *supervised person's* business.

67. The *MLCO* may have a functional reporting line, e.g., to a group compliance function.

68. The *Money Laundering Order* does not rule out the possibility that the *MLCO* may also have other responsibilities. To the extent that the *MLCO* is also responsible for the development of *systems and controls* (and *policies and procedures*), as well as monitoring subsequent compliance with those *systems and controls* (and *policies and procedures*), some additional independent assessment of compliance will be needed from time to time to address this conflict of interest. Such an independent assessment is unlikely to be needed where the role of the *MLCO* is limited to actively monitoring the development and implementation of such *systems and controls*.

Statutory requirements (paraphrased wording)

69. *Article 7 of the Money Laundering Order requires a relevant person or the relevant person's AMLSP, where applicable, to appoint a MLCO to monitor whether the enactments in Jersey relating to money laundering and the financing of terrorism and AML/CFT/CPF Codes of Practice are being complied with. The same person may be appointed as both MLCO and MLRO.*

70. *Article 7(2A) of the Money Laundering Order requires a relevant person to ensure that the individual appointed is of an appropriate level of seniority and has timely access to all records that are necessary or expedient.*

71. *Article 7(6) of the Money Laundering Order requires a relevant person to notify the JFSC in writing within one month when a person is appointed as, or ceases to be, a MLCO. However, Article 10 of the Money Laundering Order provides that the JFSC may grant exemptions from this notification requirement, by way of notice.*

72. *Article 7 of the Money Laundering Order recognises that a relevant person that is also a regulated person may have notified the JFSC of the appointment or cessation of a MLCO under other legislation. If so, a duplicate notification is not required under the Money Laundering Order.*

AML/CFT/CPF Codes of Practice

[COP18] A *supervised person* must appoint an *MLCO* that:

› subject to Article 9A (Appointment of *AMLSP* to fulfil obligations of *relevant person*) is employed by the *supervised person* or an enterprise in the same *financial group* as the *supervised person;*

  i) In the case of a *supervised person* that: carries on the business of being a functionary, recognized fund, or unclassified fund or is a Category B insurance permit holder, a managed bank, or managed entity (meaning a person carrying on *regulated business* that includes a managed trust company and an entity that is managed by a manager of a managed entity registered to carry on class ZK of fund services business); has no *employees* of its own; and is administered by a person carrying on a *regulated business*, it is acceptable for an *employee* of the administrator to be appointed by the *supervised person* as its *MLCO*;

› is based in Jersey;

  i) In the case of a *supervised person* that is a Category A insurance business permit holder with no *employees* of its own in Jersey, it is acceptable to appoint an *employee* outside Jersey. In the case of a *supervised person* that is carrying on *MVTS* activity and has no *employees* of its own in Jersey, it is acceptable for the *supervised person* to appoint an *employee* outside Jersey as its *MLCO*, provided the *employee* is based in an equivalent jurisdiction; and

› has sufficient experience and skills.

[COP19] A *supervised person* must ensure that the *MLCO*:

› has appropriate independence, in particular from *customer*-facing, business development and *systems and controls* development roles;

› reports regularly and directly to the board and has a sufficient level of authority within the *supervised person* so that the board reacts to and acts upon reports made by the *MLCO;*

› has sufficient resources, including sufficient time and (if appropriate) a *deputy MLCO* and any other persons to support them if necessary, in carrying out their responsibilities.

› is fully aware of both their and the *supervised person*'s obligations under the Anti-*Money laundering* and Counter-Terrorism Legislation and *AML/CFT/CPF Codes of Practice* issued under the Supervisory Bodies Law.

[COP20] If the position of *MLCO* is expected to fall vacant, to comply with the *statutory requirement* to have an individual appointed to the office of *MLCO* at all times, a *supervised person* must take action to appoint a member of the board (or other appropriate member of senior management) to the position on a temporary basis.

[COP21] If temporary circumstances arise where the *supervised person* has a limited or inexperienced *money laundering, terrorist financing, proliferation financing* compliance resource, it must ensure that this resource is supported as necessary.

[COP22] When considering whether it is appropriate to appoint the same person as *MLCO* and *MLRO*, a *supervised person* must have regard to:

› the respective demands of the two roles, taking into account the size and nature of the *supervised person's* activities; and

› whether the individual will have sufficient time and resources to fulfil both roles effectively.

Guidance notes

73. A *supervised person* may demonstrate that its *MLCO* is monitoring whether enactments and *AML/CFT/CPF Codes of Practice* issued under the *Supervisory Bodies Law* are being complied with where they:

› regularly monitor and test compliance with *systems and controls* (including *policies and procedures*) in place to prevent and detect *money laundering,* counter the *financing of terrorism, and* counter the *financing of proliferation* – supported as necessary by a compliance or internal *audit* function;

› report periodically, as appropriate, to the board on compliance with the *supervised person's systems and controls* (including *policies and procedures*) and issues that need to be brought to its attention;

› respond promptly to requests for information made by the *JFSC* and the *FIU*.

74. In a case where the *MLCO* is also responsible for the development of *systems and controls* (including *policies and procedures*) in line with evolving requirements, a *supervised person* may demonstrate that the *MLCO* has appropriate independence where such *systems and controls* are subject to periodic independent scrutiny.

75. Vacancy of *MLCO* as referred to in COP20 above may also apply in the event the *MLCO* is temporarily unable to fulfil his or her responsibilities, for example due to medical leave.

2.7 The *MLRO*

Overview

76. Whilst the *Money Laundering Order* requires one individual to be appointed as *MLRO* by the *supervised person* or the *supervised persons AMLSP*, where applicable (see section 15 of *this Handbook*), it recognises that, given the size and complexity of operations of many enterprises, it may be appropriate to designate additional persons (*Deputy MLROs*) to whom *SARs* may be made.

Statutory requirements (paraphrased wording)

77. *Article 8 of the Money Laundering Order requires a relevant person or the relevant person's AMLSP, where applicable, to appoint a MLRO. The MLRO's function is to receive and consider internal SARs in accordance with internal reporting procedures. The same person may be appointed as both MLCO and MLRO.*

78. *Article 8(2A) of the Money Laundering Order requires a relevant person to ensure that the individual appointed is of an appropriate level of seniority and has timely access to all records that are necessary or expedient.*

79. *Article 8(4) of the Money Laundering Order requires a relevant person to notify the JFSC in writing within one month when a person is appointed as, or ceases to be, a MLRO. However, Article 10 provides that the JFSC may grant exemptions from this notification requirement, by way of notice.*

80. *Article 8 of the Money Laundering Order recognises that a relevant person that is also a regulated person may have notified the JFSC of the appointment or cessation of a MLRO under other legislation. If so, a duplicate notification is not required under the Money Laundering Order.*

81. *Article 9 of the Money Laundering Order allows a relevant person to designate one or more Deputy MLROs, in addition to the MLRO, to whom internal SARs may be made.*

AML/CFT/CPF Codes of Practice

[COP23] A *supervised person* must appoint a *MLRO* that, subject to Article 9A of the *Money Laundering Order* (Appointment of *AMLSP* to fulfil obligations of *relevant person*):

- is employed by the *supervised person* or enterprise in the same *financial group* as the *supervised person;*
    i) In the case of a *supervised person* that: carries on the business of being a functionary, recognized fund, or unclassified fund, or is a Category B insurance permit holder, a managed bank, or managed entity (meaning a regulated business that includes a managed trust company and an entity that is managed by a manager of a managed entity registered to carry on class ZK of fund services business); has no employees of its own; and is administered by a person carrying on regulated *business* that is a *supervised person*, it is acceptable for an *employee* of the administrator to be appointed by the *supervised person* as its *MLRO*;
- is based in Jersey;

    In the case of a *supervised person* that is a Category A insurance business permit holder with no employees of its own in Jersey, it is acceptable to appoint an employee outside Jersey In the case of a *supervised person* that is carrying on MVTS activity and has no employees of its own in Jersey, it is acceptable for the *supervised person* to appoint an employee outside Jersey as its *MLRO*, provided the employee is based in an equivalent jurisdiction; and
- has sufficient experience and skills.

[COP24] A *supervised person* must ensure that the *MLRO*:

- has appropriate independence, in particular from *customer*-facing and business development roles;
- has a sufficient level of authority within the *supervised person;*

› has sufficient resources, including sufficient time, and (if appropriate) is supported by *Deputy MLROs;*

› is able to raise issues directly with the board; and

› is fully aware of both their and the *supervised person's* obligations under the *Anti Money Laundering and Counter Terrorism Legislation* and the *AML/CFT/CPF Codes of Practice* issued under the Supervisory Bodies Law.

[COP25] Where a *supervised person* has appointed one or more *Deputy MLROs* the requirements set out above for the *MLRO* must also be applied to any *Deputy MLROs*.

[COP26] Where a *supervised person* has appointed one or more *Deputy MLROs*, it must ensure that the *MLRO*:

› keeps a record of all *Deputy MLROs;*

› provides support to, and routinely monitors the performance of, each *Deputy MLRO;*

› considers and determines that *SARs* are being handled in an appropriate and consistent manner.

[COP27] If the position of *MLRO* is expected to fall vacant, to comply with the statutory requirement to have an individual appointed to the office of *MLRO* at all times, a *supervised person* must take action to appoint a member of the board (or other appropriate member of senior management) to the position on a temporary basis.

[COP28] If temporary circumstances arise where a *supervised person* has a limited or inexperienced *money laundering*, *terrorist financing* and *proliferation financing* reporting resource, it must ensure that this resource is supported as necessary.

Guidance notes

82. A *supervised person* may demonstrate that its *MLRO* (and any *Deputy MLRO*) is receiving and considering *SARs* in accordance with Article 21 of the *Money Laundering Order* where, among other things, its *MLRO*:

› maintains a record of all requests for information from law enforcement authorities and records relating to all internal and external *SARs* (see Section 9 of *this Handbook*);

› manages relationships effectively post disclosure to avoid tipping off any external parties;

› acts as the liaison point with the *JFSC* and the *FIU* and in any other external enquiries in relation to *money laundering*, the *financing of terrorism or proliferation financing*.

83. A *supervised person* may demonstrate routine monitoring of the performance of any Deputy *MLRO*s by requiring the *MLRO* to review:

› samples of records containing internal *SARs* and supporting information and documentation;

› decisions of the *Deputy MLRO* concerning whether to make an external *SAR;*

› the basis for decisions taken.

84. Vacancy of *MLRO* as referred to in COP27 above may also apply in the event the *MLRO* is temporarily unable to fulfil his or her responsibilities, for example due to medical leave.

2.8 *Financial groups*

Overview

85. A *financial group* of which a *supervised person* is a member must maintain a group programme for the sharing of *AML/CFT/CPF* information.

86. In addition, as explained in Section 1.4.3 of *this Handbook*, where a company incorporated in Jersey (a *supervised person*) carries on a *supervised business* through an overseas branch, it must comply with *AML/CFT/CPF Codes of Practice* issued under the *Supervisory Bodies Law* in respect of that business, irrespective of whether it also carries on *supervised business* in or from within Jersey.

87. In practice, the above only applies to *supervised persons* that meet the definition of a *financial group*, this includes a requirement that a parent company or other legal person exercise control over every member of that group for the purposes of applying group supervision.

Group supervision refers to (a) the core principles for effective banking supervision published by the *Basel Committee on Banking Supervision*; (b) the *Objectives and Principles of Securities Regulation* issued by the *International Organisation of Securities Commissions*; or (c) the Insurance Supervisory Principles issued by the *International Association of Insurance Supervisors.*

Statutory requirements (paraphrased wording)

88. *Article 11A of the Money Laundering Order applies to financial groups and/or DNFBPs of which a relevant person is a member.*

89. *Article 11A(2) of the Money Laundering Order requires a financial group to maintain a programme to prevent and detect money Laundering and the financing of terrorism that includes:*

- *Policies and procedures by which a relevant person within a financial group, which carries on financial services business or equivalent business, may disclose information to a member of the same financial group, but only where such disclosure is appropriate for the purpose of preventing and detecting money laundering or managing money laundering risks;*
- *Adequate safeguards for the confidentiality and use of any such information;*
- *The monitoring and management of compliance with, and the internal communication of, such policies and procedures (including the appointment of a Compliance Officer for the financial group);*
- *The screening of employees.*

90. *Under Article 11A(3) of the Money Laundering Order "information" includes the following:*

- *Information or evidence obtained from applying identification measures;*
- *Customer, account, and transaction information;*
- *Information relating to the analysis of transactions or activities that are considered unusual.*

91. *Under Article 11A(4) "financial groups" includes a group of persons falling within Part 3 of* Schedule 2 *of the Law (designated non-financial businesses and professions) if there is, in relation to the group, a parent company or other legal person that exercises control over every member of the group.*

AML/CFT/CPF Codes of Practice

[COP29] A *supervised person* that is a Jersey incorporated company must ensure that any subsidiary applies measures that are at least equivalent to the *AML/CFT/CPF Codes of Practice* in respect of any *supervised business* carried on outside Jersey by that subsidiary.

[COP30] A *supervised person* who:

- is registered, incorporated or otherwise established under Jersey law, but who is not a Jersey incorporated company; and
- carries on a *supervised business* in or from within Jersey,

must apply measures that are at least equivalent to the *AML/CFT/CPF Codes of Practice* in respect of any *supervised business* carried on by that person through an overseas branch/office.

[COP31] A person who:

- is registered, incorporated or otherwise established under Jersey law, but who is not a Jersey incorporated company; and
- carries on a *supervised business* in or from within Jersey,

must ensure that any subsidiary applies measures that are at least equivalent to the *AML/CFT/CPF Codes of Practice* in respect of any *supervised business* carried on outside Jersey by that person.

[COP32] Where overseas legislation prohibits compliance with an *AML/CFT/CPF Code of Practice* (or measures that are at least equivalent) then the *AML/CFT/CPF Codes of Practice* do not apply and the *JFSC* must be informed that this is the case. In such circumstances, a *supervised person* must take other reasonable steps to effectively deal with the risk of *money laundering*, the *financing of terrorism*, and the *financing of proliferation*.

Guidance notes

92. A *financial group's* policies and procedures governing disclosure of information between members of the *financial group* (as required by Article 11A(2) of the *Money Laundering Order*) should address, in particular:

- provision by *supervised persons* to group-level compliance, *audit*, and/or *AML/CFT/ CPF* functions of *customer*, account, and transaction information when necessary for *AML/CFT/CPF* purposes, which should include information and analysis of transactions or activities which appear unusual and could include a *SAR,* its underlying information, or the fact that a *SAR* has been submitted, as permitted by Article 22A of the *Money Laundering Order* (see Section 9.6 of *this Handbook*);
- provision from these group-level functions to the *supervised person* when relevant and appropriate to risk management; and
- provision of information between members of the group for *CDD* purposes.

3 *IDENTIFICATION MEASURES* – OVERVIEW

3.1 Overview of section

1. This section explains the *identification measures* required under Article 13 of the *Money Laundering Order*, and the framework under which a *supervised person* is required to apply a risk-based approach to the application of such measures.

2. This section should be read and understood in conjunction with the following sections:

- Section 4 of *this Handbook* – which explains the basis for finding out identity and obtaining evidence of identity;
- Section 5 of *this Handbook* – which considers the circumstances in which reliance might be placed on another party to have applied *reliance identification measures*;
- Section 6 of *this Handbook* – which explains the ongoing requirements to monitor relationships on an ongoing basis;
- Section 7 of *this Handbook* – which explains the application of *enhanced CDD measures* (including the case of a *customer* that is assessed as presenting a higher risk); and
- Section 8 of *this Handbook* – which explains the application of simplified *identification measures*.

3. Sound *identification measures* are vital because they:

- help to protect the *supervised person* and the integrity of the financial sector in which it operates by reducing the likelihood of the business becoming a vehicle for, or a victim of, *financial crime*, including *money laundering,* the *financing of terrorism,* and the *financing of proliferation*;
- assist law enforcement, by providing available information on *customers* or activities and transactions being investigated;
- constitute an essential part of sound risk management, e.g., by providing the basis for identifying, limiting and controlling risk;
- help to guard against identity fraud.

4. The inadequacy or absence of *identification measures* can expose a *supervised person* to serious *customer* and counterparty risks, as well as reputational, operational, legal, regulatory and concentration risks, any of which can result in significant financial cost to the business. Documents, data, or information held also assist the *MLRO* (or *Deputy MLRO*) and other employees to determine whether a *SAR* is appropriate.

5. A *customer* may be an individual (or group of individuals) or legal person. Section 4.2.1 of *this Handbook* deals with a *customer* who is an individual (or group of individuals), Section 4.3 of *this Handbook* deals with a *customer* (an individual or legal person) who is acting for a legal arrangement, and Section 4.5 of *this Handbook* deals with a *customer* who is a legal person.

6. The term *customer*, as used in *this Handbook*, is defined in the Glossary of *this Handbook*. As noted in the definition, *customers* can include a prospective *customer* (i.e., applicants for business).

3.2 Obligation to apply *identification* measures

Statutory requirements (paraphrased wording)

7. *Article 13(1) of the Money Laundering Order requires a relevant person to apply CDD measures. CDD measures comprise identification measures and ongoing monitoring. Identification measures must be applied:*

- *subject to Article 13(4) to (11) of the Money Laundering Order, before the establishment of a business relationship or before carrying out a one-off transaction;*
- *where a relevant person suspects money laundering;*
- *where a relevant person has doubts about the veracity of documents, data or information previously obtained under CDD measures.*

<u>Identification Measures</u>

8. *Article 3(2) of the Money Laundering Order sets out what identification measures are to involve:*

- *finding out the identity of a* ***customer*** *and obtaining evidence of identity from a reliable and independent source that is reasonably capable of verifying that the person to be identified is who the person is said to be and satisfies the person responsible for the identification of a person that the evidence does establish that fact (referred to as "****obtaining evidence****"). See Article 3(2)(a) of the Money Laundering Order;*
- *finding out the identity of any person purporting to act on behalf of the customer and verifying the authority of any person purporting so to act. See Article 3(2)(aa) of the Money Laundering Order;*
- ***where the customer is a legal person****, understanding the ownership and control structure of that customer and the provisions under which the customer can enter into contracts, or other similarly legal binding arrangements, with third parties. See Article 3(2)(c)(ii) of the Money Laundering Order;*
- ***where the customer is a legal person****, finding out the identity of individuals who are the beneficial owners or controllers of the customer and obtaining evidence of the identity of those individuals. See Article 3(2)(c)(iii) of the Money Laundering Order;*
- *determining whether the customer is acting for a third party (or parties), whether directly or indirectly. See Article 3(2)(b) of the Money Laundering Order;*
- *finding out the identity of any* ***third party*** *(or parties) on whose behalf the customer is acting and obtaining evidence of the identity of those persons. See Article 3(2)(b)(i) of the Money Laundering Order;*
- ***where the third party is a legal person****, understanding the ownership and control of that third party, finding out the identity of the individuals who are the beneficial owners or controllers of the third party and obtaining evidence of the identity of those individuals. See Article 3(2)(b)(ii) of the Money Laundering Order;*
- ***where the third party is a legal arrangement****, e.g., a trust, understanding the nature of the legal arrangement under which the third party is constituted. See Article 3(2)(b)(iii)(A) of the Money Laundering Order;*

- ***where the third party is a legal arrangement**, e.g., a trust, finding out the identity of the persons who are listed in Article 3(7) of the Money Laundering Order. See Article 3(2)(b)(iii)(B) of the Money Laundering Order;*
- ***where the third party is a legal arrangement**, e.g., a trust, where any person listed in Article 3(7) is not an individual, finding out the identity of the individuals who are the beneficial owners or controllers of the person and obtaining evidence of the identity of those individuals. See Article 3(2)(b)(iii)(C) of the Money Laundering Order;*
- *obtaining information on the purpose and intended nature of the business relationship or one-off transaction. See Article 3(2)(d) of the Money Laundering Order.*

9. *Article 3(5) of the Money Laundering Order requires identification measures to include the assessment (i.e., CRA) by a relevant person of the risk that a business relationship or one-off transaction will involve money laundering. This must include obtaining appropriate information for assessing that risk.*

10. *Article 3(6) of the Money Laundering Order requires, in cases where a customer is acting for a third party, and where the customer is a legal person, measures for obtaining evidence of identity for third parties, persons purporting to act on behalf of the customer, and individuals who are the customer's beneficial owners or controllers, to involve reasonable measures having regard to all the circumstances of the case, including the degree of risk assessed.*

11. *For persons who are not individuals, Article 2 of the Money Laundering Order describes:*

- *beneficial owners as individuals with ultimate beneficial ownership of that person;*
- *beneficial controllers as individuals who ultimately control that person or otherwise exercise control over the management of that person.*

12. *The description of a beneficial owner or controller will apply whether the individual satisfies the description alone or jointly with other persons.*

13. *Article 2 of the Money Laundering Order provides that no individual is to be treated as a beneficial owner of a person that is a body corporate or a limited liability company, the securities of which are listed on a regulated market.*

Ongoing Monitoring

14. *Article 3(3) of the Money Laundering Order sets out what ongoing monitoring is to involve:*

- *scrutinising transactions undertaken throughout the course of a business relationship to ensure that the transactions being conducted are consistent with the relevant person's knowledge of the customer, including the customer's business and risk profile. See Article 3(3)(a) of the Money Laundering Order;*
- *keeping documents, data, or information up to date and relevant by undertaking reviews of existing records, particularly in relation to higher risk categories of customers. See Article 3(3)(b) of the Money Laundering Order.*

Policies and procedures

15. *Among other things, Article 11(1) and (2) of the Money Laundering Order requires a relevant person to maintain policies and procedures for the application of CDD measures that are appropriate and consistent having regard to the degree of risk of money laundering and the financing of terrorism taking into account:*

- *the level of risk identified in a national or sector-specific risk assessment in relation to money laundering carried out in respect of Jersey;*

› *the type of customers, business relationships, products, and transactions with which the relevant person's business is concerned.*

16. *Among other things, Article 11(3) of the Money Laundering Order requires that the appropriate and consistent policies and procedures include policies and procedures which:*

› *determine whether a customer (and others connected to the customer) is a PEP, has a connection with a country or territory that does not apply, or insufficiently applies the FATF Recommendations, or is subject to or connected with a country, territory or organization that is subject to a call from the FATF for the application of enhanced due diligence measures;*

› *determine whether a transaction is with a person connected with a country or territory that does not apply, or insufficiently applies the FATF Recommendations, or is subject to or connected with a country, territory or organisation that is subject to a call from the FATF for the application of enhanced CDD measures;*

› *assess and manage the risk of money laundering and the financing of terrorism occurring because of completing identification measures after the establishment of a business relationship (where permitted) and ensure periodic reporting to senior management in such cases.*

17. *Article 13(10) to (12) provides that a relevant person that is a Collective investment scheme shall not be required to apply customer due diligence measures to a person that becomes a unitholder through a secondary market transaction, so long as:*

› *a person carrying on investment business has applied identification measures; or*

› *a person carrying on equivalent business to investment business has applied identification measures in line with FATF Recommendation 10.*

18. *A "secondary market" is a financial market in which previously issued units are bought and sold.*

19. *Where a relationship between a relevant person and a customer has no "element of duration" and is not a one-off transaction within the meaning of Article 4 of the Money Laundering Order, identification measures within the meaning of Article 13 of the Money Laundering Order are not required unless:*

› *the relevant person suspects money laundering or financing of terrorism; or*

› *the relevant person has doubts about the veracity or adequacy of any documents, data or information previously obtained under the CDD measures.*

3.3 Risk-based approach to *identification measures*

Overview

20. A risk-based approach to the application of *identification measures* involves several discrete stages. The overall objective is to assess the most effective and proportionate way to manage the *money laundering, terrorist financing, and proliferation financing risk* faced by a *supervised person*. While these stages are required to be incorporated into *policies and procedures*, they do not need to take place in the sequence outlined below. They may also occur simultaneously.

21. The risk assessment of a particular *customer* (i.e. the *CRA*) will determine:

› the extent of information which will be requested;

› what evidence of identity will be obtained;

- the extent to which the resulting relationship will be scrutinised; and
- how often documents, data or information held will be reviewed.

22. Section 2.3 of *this Handbook* requires the board (or where the *supervised person* is not a company, senior management) of a *supervised person* to conduct (and keep up to date) a *BRA*, which considers the *supervised person's* risk appetite, activities and structure and concludes on the *supervised person's* exposure to *money laundering*, the *financing of terrorism, and* the *financing of proliferation* risk.

23. This *BRA* will enable a *supervised person* to determine its initial approach to performing Stage 1 of the identification process as set out below, depending on the type of *customer*, product or service involved. The remaining stages of the process require a *supervised person* to consider whether the specific circumstances of the *customer* will necessitate the application of further measures.

24. Part 3A of the *Money Laundering Order* sets out exemptions from *CDD* requirements, including; circumstances in which exemptions do not apply (see Article 17A of the *Money Laundering Order*); exemptions from applying other identification requirements (see Articles 17B, 17C and 18 of the *Money Laundering Order*); and the obligations of a *supervised person* who is exempt from applying *third party identification requirements* (see Article 17D of the *Money Laundering Order*).

25. The following are the stages in the identification process:

Stage	***Identification measures***	**Article(s) of the *MLO***	**Section in *the Handbook***
1.1	In the case of a *customer* that is a legal person, a *supervised person* must understand the *ownership and control* structure of the *customer* (and provisions under which the *customer* can enter into contracts).	3(2)(c)(ii)	Section 3.3.1
1.2	A *supervised person* must find out the identity of: › the *customer*; › any *Beneficial owners and controllers* of the *customer*; › any third party (or parties) – including a legal arrangement - on whose behalf the *customer* acts. Whether directly or indirectly (and *Beneficial owners and controllers* of the third party (or parties)); o For the avoidance of doubt, the above will include any person who is a named beneficiary of a life assurance policy entered into by the *customer*. Where there is no named beneficiary and they are designated by characteristics or by class or by other means, this means obtaining sufficient information about who the beneficiaries of a life policy are, sufficient to enable an assessment of risk of the *customer* relationship and to enable beneficiaries to be identified and verified at the time of the pay-out and › others listed in Article 3(2) of the *Money Laundering Order*.	3(2)(a) to (c) 3(4)(a)	Section 4

Stage	***Identification measures***	**Article(s) of the *MLO***	**Section in *the Handbook***
1.3	A *supervised person* must obtain information on the purpose and intended nature of the *business relationship* or *one-off transaction*. Also note additional *AML/CFT/CPF Codes of Practice* requirement to **understand** purpose and intended nature.	3(2)(d)	Sections 3.3.2 and 3.3.3 Section 7
1.4	A *supervised person* must obtain appropriate information for assessing the risk that a *business relationship* or *one-off transaction* will involve *money laundering*, the *financing of terrorism,* or the *financing of proliferation*. It may be necessary to repeat this stage following an assessment of risk under stage 2.1 below.	3(5) 15(1)	Sections 3.3.2 and 3.3.3 Section 7
2.1	A *supervised person* must, based on information collected at stage 1 above, assess the risk that a *business relationship* or *one-off transaction* will involve *money laundering, the financing of terrorism,* or the *financing of proliferation* (risk profile).	3(5)	Section 3.3.4
2.2	A *supervised person* must prepare and record a *customer* business and risk profile.	3(3)(a)	Section 3.3.5
3	A *supervised person* must obtain evidence of the identity of those whose identity is found out at stage 1.2 above.	3(2)(a) to (c) 3(4)(b) 15(1)	Section 4 Section 7

26. By virtue of ongoing monitoring, particularly in relation to higher risk categories of *customers*, under Article 3(3)(b) of the *Money Laundering Order*, a *supervised person* must keep documents, data and information obtained under Stages 1 and 3 up to date and relevant. See Section 3.4 of *this Handbook*.

27. As shown in the table above, in some cases the *Money Laundering Order* requires *supervised persons* to simply obtain information. For example, finding out identity (Stage 1.2 above).

28. However, in other cases the *Money Laundering Order* requires *supervised persons* to also understand the information they obtain. For example, the ownership and control structure of the *customer* (Stage 1.1 above).

29. For each stage of the process, it is important for *supervised persons* to be aware of the distinction between factual information which they simply need to collect (name, address, date of birth, etc.) and that which requires further analysis (structure charts relating to ultimate *beneficial ownership*, publicly available adverse media, credit reports, etc.). This will assist in the identification and risk assessment process being carried out effectively.

30. *Systems and controls* (including *policies and procedures*) will not detect and prevent all instances of *money laundering*, the *financing of terrorism,* or the *financing of proliferation*. A risk-based approach will, however, serve to balance the cost burden placed on a *supervised person* and on *customers* with the risk that the business may be used in *money laundering,* the *financing of terrorism,* or the *financing of proliferation* by focusing resources on higher risk areas.

31. Care has to be exercised under a risk-based approach. Being identified as carrying a higher risk of *money laundering,* the *financing of terrorism,* or the *financing of proliferation* does not automatically mean that a *customer* is a *money launderer*, is *financing terrorism*, or is *financing proliferation*. Similarly, identifying a *customer* as carrying a lower risk of *money laundering,* the *financing of terrorism,* or the *financing of proliferation* does not mean that the *customer* is not a *money launderer*, a *terrorist financier,* or *finances proliferation* of weapons of mass destruction.

AML/CFT/CPF Codes of Practice

[COP33] A *supervised person* must apply a risk-based approach to determine the extent and nature of the measures to be taken when undertaking the identification process set out above.

[COP34] A *supervised person* must understand the purpose and intended nature of a *business relationship* or *one-off transaction.*

[COP35] A *supervised person* must understand the nature and scope of the business activities generating a *customer*'s funds/assets.

Guidance notes

32. A *supervised person* may demonstrate that it understands the nature and scope of a *customer's* business activities where it collects and considers information regarding those activities. The volume of information collected and considered should be determined on a risk-based approach and may include, but is not limited to, the following:

- › the industry sectors within which the business operates. The *supervised person* is not required to have an expert understanding of each industry sector, rather it should be sufficient to understand the potential risk exposure of the sector to *money laundering*, the *financing of terrorism*, or the *financing of proliferation*;
- › whether the business activities display any higher risk indicators of *money laundering*, the *financing of terrorism*, or the *financing of proliferation*. These include, but are not limited to, the indicators listed at paragraph 77 below;
- › whether the business is a state-owned enterprise or receives any government funding;
- › the geographical scope of the business activities. For example, where the business operates and what it does in those countries;
- › the reputation of the *customer's* business. For example, using a search engine to identify if any adverse media comment has been made on the conduct of the business and its *Beneficial owners and/or controllers*; and
- › further clarification from the *customer* regarding any of the above, where necessary.

33. When undertaking the above activities, a *supervised person* should document their consideration (i.e., their thought process) and record their conclusions.

34. Where information is provided by someone other than the *customer* themselves, additional questions may need to be asked to assess whether it is reasonable to use this information, and consideration of the *AML/CFT/CPF* risk should be undertaken as part of the CRA.

3.3.1 Understanding ownership structure – Stage 1.1

Overview

35. Article 3(2)(c)(ii) of the *Money Laundering Order* requires a *supervised person* to understand who owns and controls a *customer* that is a legal person. Without such an understanding, it will not be possible to identify the individuals who are the *customer*'s *Beneficial owners and/or controllers*.

36. Understanding ownership involves taking three separate steps:

› requesting information from the *customer* (or a professional);

› validating that information;

› checking that information held makes sense.

Guidance notes

37. **Step 1** – A *supervised person* may demonstrate that it understands the ownership and control structure of a *customer* that is a legal person where it applies one of the following *identification measures*:

› it requests the *customer* to provide a statement of legal and *Beneficial ownership and control* as part of its application to become a *customer*. In the case of a legal person that is part of a group, this will include a group structure;

› to the extent that a *customer* is, or has been, provided with professional services by a *Lawyer* or *Accountant*, or is "administered" by a *TCSP*, it requests that *Lawyer*, *Accountant* or *TCSP* provide a statement of legal and *Beneficial ownership and control*. In the case of a legal person that is part of a group, this will include a group structure.

38. Where there is a reason to doubt the accuracy, or veracity of the statement or where higher risk factors are present, a *supervised person* who has been provided with a statement of legal and *Beneficial ownership and control* from a third party such as a Lawyer, Accountant or TCSP should not accept such document/information on face value but should consider whether it is reasonable to use this document/information and factor such consideration into any risk assessment undertaken.

39. **Step 2** – A *supervised person* may demonstrate that it understands the **legal** *ownership and control* structure of a *customer* that is a legal person where it considers information that is held:

› by the *customer*, e.g. recorded in its share register;

› by a *Lawyer*, *Accountant* or *TCSP*;

› by a trusted external party, in the case of a legal person with bearer shares, where bearer certificates have been lodged with that trusted external party;

› publicly, e.g., information that is held in a central register in the country of establishment.

40. A *supervised person* may demonstrate that it understands the ***Beneficial*** *ownership and control* structure of a *customer* that is a legal person where it considers information that is:

› held by the *customer*, e.g., in line with the *Company Law*, *AML/CFT/CPF* requirements, or listing rules, e.g., a declaration of trust in respect of shares held by a nominee shareholder;

› held by a *Lawyer, Accountant* or *TCSP*, e.g., in order to meet *AML/CFT/CPF* requirements;

› held in a public register, e.g., information that is held in a central register of *beneficial ownership* in the country of establishment, information that is published in financial statements prepared under generally accepted accounting principles, or information available as a result of a listing of securities on a stock exchange;

› provided directly by the ultimate *beneficial owner(s)* of the legal person;

› publicly available, e.g., in commercial databases and press reports.

41. **Step 3** – A *supervised person* may demonstrate that it understands the *ownership and control* structure of a *customer* that is a legal person where it applies one or more of the following *identification measures*:

- › it considers the purpose and rationale for using an entity with a separate legal personality;
- › in the case of a legal person that is part of a group, it considers whether the corporate structure makes economic sense, considering complexity and multi-jurisdictional aspects.

3.3.2 Information for assessing risk – Stage 1.4

Guidance notes

42. A *supervised person* may demonstrate that it has obtained appropriate information for assessing the risk that a *business relationship* or *one-off transaction* will involve *money laundering,* the *financing of terrorism,* or the *financing of proliferation* where it collects the following information:

All *customer* types	
All *customer* types	› Type, volume and value of activity expected (having regard for the *JFSC's* Sound Business Policy). › *Source of funds*, e.g., nature and details of occupation or employment. › Details of any existing relationships with the *supervised person*.

Additional relationship information	
Express trusts	› Type of trust (e.g., fixed interest, discretionary, testamentary). › Classes of beneficiaries, including any charitable causes named in the trust instrument.
Foundations	› Classes of beneficiaries, including any charitable objects.
Legal persons and legal arrangements (including *express trusts* and foundations)	› Ownership structure of any underlying legal persons. › Type of activities undertaken by any underlying legal persons (having regard for the *JFSC's* Sound Business Policy and trading activities). › Geographical sphere of activities and assets. › Name of regulator, if applicable.

43. The extent of information sought in respect of a particular *customer*, or type of *customer*, will depend upon the country, territory or area with which the *customer* is connected, the characteristics of the product or service requested, how the product or service will be delivered, as well as factors specific to the *customer*.

3.3.2.1 Terms of business

Overview

44. It may be helpful to:

- › explain to the *customer* the reason for requiring *CDD* information and for the *customer* identification procedures. This can be achieved by including an additional paragraph in the terms of business or in pre-engagement communications.

› inform *customers* of the *supervised person's* reporting responsibilities under the primary legislation and the restrictions created by the 'tipping-off' rule on the *supervised person's* ability to discuss such matters with its *customers*.

45. Whether or not to advise the *customer* of these issues is a decision to be taken by individual *supervised persons*. However, if it is to be done it is important that the policy should apply consistently for all *customers*. A decision only to do so once a suspicion has arisen could result in the *supervised person* committing a tipping-off offence (see Section 9.5 of *this Handbook*).

3.3.2.2 **Issues that might be covered when drawing up a profile**

Guidance notes

46. To assist in drawing up a *customer* profile, *supervised persons* may wish to obtain information via a questionnaire. *Supervised persons* should be mindful that the questionnaire requests information they are legally obligated to obtain. *Supervised persons* should amend the questions and focus to suit their own *customer* base and products/services offered.

47. The *supervised person* may also be able to obtain further information prior the start of a *business relationship* or *one-off transaction* from other sources. Examples include:

› carrying out background searches and database screening; and

› communicating with existing or previous providers of professional accountancy, banking, and legal services to the *customer*.

3.3.3 Source of funds – Stage 1.4

Overview

48. The ability to follow the audit trail for criminal funds and transactions flowing through the professional and financial sector is a vital law enforcement tool in *money laundering,* the *financing of terrorism,* and the *financing of proliferation* investigations. Understanding the *source of funds* and, in higher risk relationships, the *customer*'s *source of wealth* is also an important aspect of *CDD*.

49. *Source of funds* is defined in the Glossary *of this Handbook*. Information concerning the geographical sphere of the activities generating the *source of funds* may also be relevant.

50. *Supervised persons* should monitor whether funds received from *customers* are from credible sources. If funding is from a source other than a *customer*, a *supervised person* may need to make further enquiries. If it is decided to accept funds from a third party, perhaps because time is short, *supervised persons* should ask how and why the third party is helping with the funding.

51. In some circumstances, cleared funds will be essential for transactions and *customers* may want to provide cash to meet a deadline. *Supervised persons* should assess the risk in these cases and ask more questions if necessary.

52. The *Money Laundering Order* and the *AML/CFT/CPF Handbook* stipulate record-keeping requirements for transaction records. These require information concerning the remittance of funds to be recorded (e.g., the name of the bank and the name and account number of the account from which the funds were remitted). This remittance information is the source of transfer and not to be confused with *source of funds* information.

53. *Source of wealth* is defined in the Glossary of *this Handbook*. It should also be reiterated that *source of wealth* is distinct from *source of funds*. Information concerning the geographical sphere of the activities that have generated a *customer's* wealth may also be relevant.

54. In finding out a *customer's source of wealth* it may not be necessary to determine the monetary value of their net worth.

3.3.4 Assessment of risk – Stage 2.1

55. The following factors - country risk, product/service risk, delivery risk, and *customer*-specific risk - will be relevant when assessing and evaluating the *CDD* information collected at Stage 1 and are not intended to be exhaustive. A *supervised person* should consider whether other variables are appropriate factors to consider in the context of the products and services that it provides and its *customer* base.

56. In assessing *customer* risk, the presence of one factor that might indicate higher risk will not automatically mean that a *customer* is in fact higher risk. Equally, the presence of one lower risk factor should not automatically lead to a determination that a *customer* is lower risk.

57. The sophistication of the risk assessment process may be determined according to factors supported by the *BRA*.

58. Inconsistencies between information obtained may also assist in assessing risk. For example, a *supervised person* might identify inconsistencies between specific information concerning *source of funds* (or *source of wealth*), and the nature of the *customer's* expected activity.

59. A *supervised person* may demonstrate that it has assessed the risk that a *business relationship* or *one-off transaction* will involve *money laundering*, the *financing of terrorism,* or the *financing of proliferation* where it considers the factors set out at Section 3.3.4.1 of *this Handbook*.

60. A *supervised person* may demonstrate that it has assessed the risk that a *business relationship* or *one-off transaction* will involve *money laundering*, the *financing of terrorism,* or the *financing of proliferation* where it considers other factors that are relevant in the context of the products and services that it provides and its *customer* base.

61. A *supervised person* may demonstrate that it has assessed the risk that a *business relationship* or *one-off transaction* will involve *money laundering,* the *financing of terrorism,* or the *financing of proliferation* where it takes into account the effect of a combination of several factors – e.g. the use of complex structures by a *customer* who is a non-resident high-net-worth individual making use of wealth management services – which may increase the cumulative level of risk beyond the sum of each individual risk element. The **accumulation of risk** is itself a factor to consider.

62. A *supervised person* may demonstrate that it has assessed the risk that a business relationship or one-off transaction will involve *money laundering*, the *financing of terrorism*, or *proliferation financing* where it takes into account the potential effect of the person or persons collating the *CDD* of the *customer* being a third party, e.g. they might be twice or even further removed from the *supervised person.*

63. Notwithstanding the above, where it is appropriate to do so, a *supervised person* may demonstrate that it has assessed the risk that a *business relationship* or *one-off transaction* will involve *money laundering,* the *financing of terrorism,* or the *financing of proliferation* where it assesses that risk "generically" for *customers* falling into similar categories. For example:

- the business of some *supervised persons*, their products, and *customer* base, can be relatively simple, involving few products, with most *customers* falling into similar risk categories. In such circumstances a simple approach, building on the risk that the *supervised person's* products are assessed to present, may be appropriate for most *customers*, with the focus being on those *customers* who fall outside the norm;
- other *supervised persons* may have a greater volume of business, but large numbers of their *customers* may be predominantly "retail", served through delivery channels that offer the

possibility of adopting a standardised approach to many procedures. Here too, the approach for most *customers* may be relatively straight forward - building on product risk;

› in the case of Jersey residents seeking to establish retail relationships, and in the absence of any information to indicate otherwise, such *customers* may be considered to present a lower risk.

3.3.4.1 Factors to consider

64. **Country Risk** – A connection to a country, territory or area that presents a higher risk of *money laundering*, the *financing of terrorism*, or the *financing of proliferation*. The following types of countries, territories or areas may be considered to present a higher risk (non-exhaustive):

› those with strategic deficiencies in the fight against *money laundering,* the *financing of terrorism,* and the *financing of proliferation*, e.g., those identified by the *FATF* as having strategic deficiencies:

  - when the *FATF* places jurisdictions under increased monitoring where they are identified as having strategic deficiencies. The list of jurisdictions under increased monitoring which **have committed** to addressing their issues is often informally referred to as *FATF's* "grey list". Jurisdictions which **do not** have an action plan are placed on a list of high-risk jurisdictions subject to a call for action. This is informally known as *FATF's* "black list";
  - where a *customer* has a connection to a country on the *FATF's grey list* or *black list*, such as a portion of their *source of wealth* originating from that country, it is possible they may try to disguise or obscure that connection to avoid additional scrutiny. *Supervised persons* should be mindful of *customers* whose *source of wealth* is routed through multiple intermediate layers, and seek to understand the ultimate geographic origin of the *source of wealth*;
  - up-to-date versions of both the *FATF's* grey list and black lists are maintained on the *FATF* website.

› those identified as major illicit drug producers, or through which significant quantities of drugs are transited, e.g., those listed by the US Department of State in its annual International Narcotics Control Strategy Report;

› those that do not take efforts to confront and eliminate human trafficking, e.g., those listed in Tier 3 of the US Department of State's annual Trafficking in Persons Report;

› those that have strong links (such as funding or other support) with *terrorist activities*, e.g. those designated by the US Secretary of State as State sponsors of terrorism; and those physical areas identified by the US (in its annual report entitled Country Reports on Terrorism) as ungoverned, under-governed or ill-governed where *terrorists* are able to organise, plan, raise funds, communicate, recruit, train, transit and operate in relative security because of inadequate governance capability, political will or both;

› those that are involved in the proliferation of nuclear and other weapons, e.g., those that are the subject of sanctions measures in place in Jersey, or, as appropriate, elsewhere;

› those that are vulnerable to corruption, e.g., those with poor ratings in Transparency International's Corruption Perception Index or highlighted as a concern in the Worldwide Governance Indicators project;

  i) when considering the level of corruption risk in a country, it is important to consider the wider context of any issues affecting the country which may increase that risk. As noted below, this may include there being an ineffective government, or political instability;

ii) the level of corruption risk may increase where the *customer* is a *PEP*. *Supervised persons* should therefore consider how much influence their *customer* deploys in that country and assess the risk that their *source of wealth* has been tainted by the proceeds of corruption;

- those in which there is no, or little, confidence in the rule of law, in particular the quality of contract enforcement, property rights, the police and the courts, e.g., those highlighted as a concern in the Worldwide Governance Indicators project;
- those in which there is no, or little, confidence in government effectiveness, including the quality of the civil service and the degree of its independence from political pressures, e.g., those highlighted as a concern in the Worldwide Governance Indicators project;
- those that are politically unstable, e.g., those highlighted as a concern in the Worldwide Governance Indicators project, or which may be considered to be a "failed state", e.g., those listed in the Failed State Index (central government is so weak or ineffective that it has little practical control over much of its territory; non-provision of public services; widespread corruption and criminality; refugees and involuntary movement of populations; sharp economic decline);
- those that are the subject of sanctions measures that are in place in Jersey or elsewhere, e.g., those dealing with the abuse of human rights of misappropriation of State funds;
- those that lack transparency, or which have excessive secrecy laws, e.g. those identified by the *OECD* as having committed to internationally agreed tax standards, but which have not yet implemented those standards;
- those with inadequate regulatory and supervisory standards on international cooperation and information exchange, e.g., those identified by the Financial Stability Board as just making material progress towards demonstrating sufficiently strong adherence, or being non-cooperative, where it may not be possible to investigate the provenance of funds introduced into the financial system.

65. In addition to the above, *supervised persons* should also consider whether a *customer* has a *relevant connection* to a country or territory named in **Appendix D1** of *this Handbook* (countries or territories for which a *FATF* call for action applies), as well as those that are generally considered to be un-cooperative in the fight against *money laundering,* the *financing of terrorism,* and the *financing of proliferation*.

66. **Country risk** – A connection to a country, territory or area that presents a lower risk of *money laundering,* the *financing of terrorism,* or the *financing of proliferation*. The following factors may be indicative of lower risk:

- a favourable rating in the Worldwide Governance Indicators project;
- the application of national financial reporting standards that follow international financial reporting standards, e.g., those countries identified by the European Commission as having generally accepted accounting principles that are equivalent to International Financial Reporting Standards;
- a commitment to **international export control regimes** (Missile Technology Control Regime, the Australia Group, the Nuclear Suppliers Group, Wassenaar Arrangement and the Zangger Committee);

› a favourable assessment by the Financial Stability Board concerning adherence to regulatory and supervisory standards on international cooperation and information exchange;

› familiarity of a *supervised person* with a country, territory or area, including knowledge of its local legislation, regulations and rules, as well as the structure and extent of regulatory oversight, for example as a result of a *supervised person's* own or group operations within that country, territory or area.

67. **Product or service risk** – Features that may be attractive to money launderers or those financing terrorism or proliferation of weapons of mass destruction:

› ability to make payments to, or receive funds from, external parties;

› ability to pay in or withdraw cash;

› ability to migrate from one product or service to another;

› use of numbered accounts (without reference to the name of the *customer*);

› ability to use "hold mail" facilities and "care of" addresses which are not temporary arrangements;

› ability to place funds in client, pooled, nominee or other accounts, where funds are mingled with those of other persons;

› ability to place sealed parcels or sealed envelopes in safe custody boxes.

68. **Product or service risk** – Features that may indicate a higher risk of *money laundering,* the *financing of terrorism,* or the *financing of proliferation*:

› work which is outside the *supervised person's* normal range of expertise – the *money launderer* might be targeting the *supervised person* to avoid answering too many potentially revealing questions.

69. Instructions that are unusual in themselves or that are unusual for the *supervised person,* or the *customer* may give rise to concern, particularly where no rational or logical explanation can be given. Additional service area vulnerabilities and risk factors specific to certain types of *supervised business* are set out in the sector-specific Sections 12 - 21 of *this Handbook*.

70. When assessing product or service risk, it is important not to restrict the assessment to the specific services being provided by the *supervised person* to the *customer*. For example, whilst the *supervised person* may only provide services regarding the portion of a *customer*'s wealth based in the *UK*, the *customer* themselves may also have diverse, volatile holdings in higher-risk jurisdictions and carry out activities considered to be more exposed to *money laundering*, *terrorist financing*, or *proliferation financing* risk. The wider context of the *customer's* activities should be considered.

71. In respect of the above paragraph, a *supervised person* is not required to obtain a granular list of every asset held by the *customer* globally. The information obtained should be sufficient for the *supervised person* to make an informed assessment of the risk presented by the *customer's* wider activities.

72. An additional section covering the issuance of **Prepaid Cards** and their associated risks is set out as section 14.2 of *this Handbook*.

73. **Delivery risk** – Features that may be attractive to *money launderers* or those *financing terrorism*:

› non-face to face relationships - product or service delivered exclusively by post, telephone, internet, video call etc. where there is no physical contact with the *customer*;

- indirect relationship with the *customer* - use of reliance on *obliged persons* or other third parties;
- availability of "straight-through processing" of *customer* transactions (where payments may be made electronically without the need for manual intervention by a *supervised person*).

74. ***Customer*-specific risk** – Features that may indicate whether a *customer* is a money launderer or is financing terrorism or financing proliferation:

- type of *customer*. An example would be an individual who meets any of the definitions of a *PEP*. This may (but not always) present a higher risk:
    - i) a *supervised person* should be particularly aware of the enhanced corruption risk which may be posed by 'sovereign actors'. These individuals are *PEPs* who work for or are connected to national governments and have control over pooled national funds. A common example would be the senior executive of a State-owned body which pools funds from sources like central bank reserves and export revenue, such as a sovereign wealth fund;
    - ii) engaging with a *customer* who holds a senior position in a State-owned body, or having a *business relationship* with the body itself, can pose an enhance risk of corruption. Examples of how the increased risk of corruption linked to these types of *PEPs* might crystallise include:
    - iii) if the *PEP* siphons away money which legitimately belongs to the sovereign wealth fund via a trust and company structure, for their own personal gain; or
    - iv) where the State-owned corporation itself is involved in illicit activity, as opposed to one or two 'bad actors' within the organisation. In this scenario, the corporation might utilise a structure to buy up key resources to deliberately manipulate their market price, for the benefit of the equally corrupt national government.
- nature and scope of business activities generating the funds/assets. The below examples may indicate higher risk:
    - i) a *customer* conducting "sensitive" activities (as defined by the *JFSC*'s Sound Business Policy) or conducting activities which are prohibited if carried on with certain countries;
    - ii) a *customer* engaged in higher risk trading activities (examples include, but are not limited to, trading in volatile currency pairs, assets linked to emerging market, cryptocurrencies and crypto assets);
    - iii) a *customer* engaged in business activities which fall within the Table of the *JFSC*'s Sound Business Policy;
    - iv) a *customer* engaged in a business which involves handling significant amounts of cash.
- transparency of *customer*. For example:
    - i) persons that are subject to public disclosure rules, e.g., on exchanges or *regulated markets* (or majority-owned and consolidated subsidiaries of such persons), or subject to licensing by a statutory regulator, e.g. the Jersey Competition Regulatory Authority may indicate lower risk;
    - ii) *customers* where the structure or nature of the entity or relationship makes it difficult to identify the true *Beneficial owners and controllers* may indicate higher

risk, for example those with nominee directors, nominee shareholders or which have issued bearer shares.

› behaviour by the *customer* may indicate a higher risk. For example:

  i) whilst face-to-face contact with *customers* is not always necessary or possible, an excessively obstructive or secretive *customer* may be a cause for concern;

  ii) where a *customer* requests undue levels of secrecy, a *customer* is reluctant or unwilling to provide adequate explanations or documents, or where it appears that an “audit trail” has been deliberately broken or unnecessarily layered;

  iii) where there is no commercial rationale or logical explanation for use of the products or services that are being sought;

› reputation of *customer*. For example, a well-known, reputable person, with a long history in their industry, and with abundant independent and reliable information about it and its *Beneficial owners and controllers* may indicate lower risk;

› jurisdiction of *customer*. If the *customer* is based outside Jersey, *supervised persons* will need to consider the rationale as to why the *customer* is seeking services outside of their home jurisdiction. The lack of an appropriate rationale may indicate higher risk;

› the regularity or duration of the *business relationship*. For example, longstanding *business relationships* involving frequent *customer* contact that result in a high level of understanding of the *customer* may indicate lower risk;

› type and complexity of relationship. The below examples may indicate higher risk:

  i) the use of overly complex or opaque structures with different layers of entities situated in two or more countries;

  ii) cross-border transactions involving counterparties in different parts of the world;

  iii) the unexplained use of corporate structures and *express trust*s;

  iv) the use of nominee and bearer shares;

› value of assets handled, e.g., higher value assets may indicate higher risk;

› value and frequency of cash or other “bearer” transactions (e.g., travellers’ cheques and electronic money purses), e.g., a higher value and/or frequency may indicate higher risk;

› delegation of authority by the *customer*. For example, the use of powers of attorney, mixed boards and representative offices may indicate higher risk;

› involvement of persons other than *Beneficial owners and controllers* in the operation of a *business relationship* may indicate higher risk;

› in the case of an *express trust*, the nature of the relationship between the settlor(s) and beneficiaries with a vested interest, other beneficiaries and persons who are the object of a power. For example, a trust that is established for the benefit of the close family of the settlor may indicate a lower risk;

› in the case of a life assurance policy, the identity and risk profile of any named beneficiary to the policy.

3.3.4.2 External data sources

75. In assessing the risk that countries and territories may present a higher risk, objective data published by the *IMF*, *FATF*, World Bank and the Egmont Group of Financial Intelligence Units will be relevant, as will objective information published by national governments (such as the World Factbook published by the US Central Intelligence Agency) and other reliable and independent sources, such as those referred to in Section 3.3.4.1 of *this Handbook*. Often, this information may be accessed through country or territory profiles provided on electronic subscription databases and on the internet. Some profiles, such as those available through KnowYourCountry, are free to use.

76. Information on sanctions may be found on the *JFSC's* website.

77. **Appendix D2** of *this Handbook* lists several countries, territories and areas that are identified by reliable and independent external sources as presenting a higher risk. When assessing country risk for *AML/CFT/CPF* purposes, in addition to considering the particular features of a *customer*, it will be relevant to take account of the number of occasions that a particular country, territory or area is listed for different reasons.

78. There are also several providers of country risk "league tables" that rate countries according to risk (e.g., lower, medium or higher). Some of these are free to use, e.g., KnowYourCountry and the Basel AML Index. These are based on weighted data published by external sources. Before placing reliance on country risk "league tables", care should be taken to review the methodology that has been used, including the basis followed for selecting sources, weighting applied to those sources and approach that is taken where data for a country, territory or area is missing.

79. External data sources may also assist in establishing *customer*-specific risk. For example, electronic subscription databases list individuals entrusted with prominent public functions who may therefore meet the definition of a *PEP*. The lists of sanctions designations in force in Jersey may be accessed through the *JFSC's* website.

3.3.5 *Customer* business and risk profile – Stage 2.2

80. A *supervised person* may demonstrate that it has prepared a *customer* business and risk profile where the profile enables it to:

- identify a pattern of expected transactions and activity within each *business relationship*;
- recognise unusual transactions and activity, unusually large transactions or activity, and unusual patterns of transactions or activity.

81. For certain types of products or services, a *supervised person* may demonstrate that it has prepared a *customer* business and risk profile where it does so based on generic attributes, so long as this enables it to recognise the transactions and activity referred to in the above paragraph. For more complex products or services, however, tailored profiles will be necessary.

3.4 Identification measures – taking on a book of business

Overview

82. Rather than establishing a *business relationship* directly with a *customer*, a *supervised person* may establish that relationship through the transfer of a block of *customers* from another business. The transfer may be effected through legislation or with the agreement of the *customer*.

Guidance notes

83. A *supervised person* may demonstrate that it has applied *identification measures* before establishing a *business relationship* taken on through the acquisition of a book of business where each of the following criteria are met:

- the vendor is a *supervised person* or carries on *equivalent business* (refer to section 1.8 of *this Handbook*);
- the *supervised person* has concluded that the vendor's *CDD policies and procedures* are satisfactory. This assessment must either involve sample testing or alternatively an assessment of all relevant documents, data or information for the *business relationship* to be acquired;
- before, or at the time of the transfer, the *supervised person* obtains from the vendor all the relevant documents, data or information (or copy thereof) held for each *customer* acquired.

84. When taking on *customer*s which display higher risk characteristics (e.g., connections to higher risk jurisdictions and/or a background in diverse and higher risk businesses), the *supervised person* should seek to understand the full complexity of the *customer's source of wealth*.

85. When assessing the risk level of a *customer* being taken on, it may also be necessary to consider the underlying assets held in the *customer's* portfolio and activities undertaken by any underlying entities, e.g., trading companies. Where underlying entities are present, it may be necessary for these to be subjected to screening.

86. It is not sufficient to simply transfer the business without considering the documents, data and information held for the *customer*. A judgement needs to be made, on a risk-based approach, as to whether the material provided is adequate, or if further enquiries are necessary.

87. In cases where:

- the vendor is not a *supervised person*; **or**
- the vendor is not carrying on *equivalent business* (refer to section 1.8 of *this Handbook*); **and**
- deficiencies are identified in the vendor's *CDD policies and procedures* (either at the time of transfer or subsequently),

  a *supervised person* may demonstrate that it has applied *identification measures* before establishing a *business relationship* where it determines and implements a programme to apply *identification measures* on each *customer* and remediate any deficiencies, provided the programme is agreed in advance with the *JFSC*.

4 *IDENTIFICATION MEASURES* – FINDING OUT IDENTITY AND OBTAINING EVIDENCE

4.1 Overview of section

1. This section explains what **information** on identity is to be found out when establishing a *business relationship* or carrying out a *one-off transaction* (or otherwise under Article 13 of the *Money Laundering Order*), and what **evidence** is to be obtained that is reasonably capable of verifying that the person to be identified is who they are said to be and satisfies a *supervised person* of the same.

2. This section does not address the information that must also be collected under Article 3(5) of the *Money Laundering Order* as part of *identification measures* to assess the risk that any *business relationship* or *one-off transaction* will involve *money laundering*, the *financing of terrorism*, or the *financing of proliferation*, which is covered by Stage 1.4 in section 3.3 of *this Handbook*. Nor does it address the enhanced measures that will be required to address the *case of a customer that is assessed as presenting a higher risk of money laundering, the financing of terrorism*, or the *financing of proliferation*, which is covered in section 7 of *this Handbook*.

3. Guidance is also given on the timing of obtaining evidence of identity and what to do where it is not possible to complete *identification measures*. This guidance covers all elements of *identification measures*, including, where appropriate, the collection of information under Article 3(5) of the *Money Laundering Order*.

4. The requirement to find out identity and obtain evidence (part of the *identification measures* referred to in Article 3 of the *Money Laundering Order*) applies:

- at the outset of a *business relationship* or *one-off transaction*;
- where there is suspicion of *money laundering*, or the *financing of terrorism*;
- where there is some doubt as to the veracity or adequacy of documents, data or information that are already held (including the circumstances set out in paragraph 5 below);
- in respect of "existing *customers*".

5. As stated in section 6 of *this Handbook*, the requirement to find out identity and obtain evidence will also apply when there are changes, for example:

- change in information found out for a *customer*, e.g., a change of name or change of nationality;
- change in beneficial ownership and control of a *customer*;
- change in a third party (or parties), or *beneficial ownership or control* of a third party (or parties) on whose behalf a *customer* acts.

6. A *customer* may be an individual (or group of individuals) or a legal person. Section 4.2.1 of *this Handbook* with a *customer* who is an individual (or group of individuals), section 4.3 of *this Handbook* deals with a *customer* (an individual or a legal person) who is acting for a legal arrangement, e.g., the trustee of an *express trust*, and section 4.5 of *this Handbook* deals with a *customer* who is a legal person.

7. The term *customer* is defined in the Glossary of *this Handbook* and further guidance is provided in the *Guidelines*.

4.2 Obligation to find out identity and obtain evidence

Overview

8. Determining that a *customer* is the person they claim to be is a combination of being satisfied that:

- a **person exists** - on the basis of information found out; and
- the *customer* **is that person** - by collecting from reliable and independent sources (documents, data, or information), satisfactory confirmatory evidence of appropriate components of the *customer's* identity.

9. Evidence of identity can take a number of forms. In respect of individuals, identity documents (e.g., passports and national identity cards) are often the easiest way of providing evidence as to someone's identity. It is, however, possible to be satisfied as to a *customer*'s identity by obtaining other forms of confirmation, including independent data sources, *Digital ID* (see section 4.3.5 of *this Handbook*) and, in appropriate circumstances, written assurances from *obliged person*s.

10. When obtaining evidence of identity, a *supervised person* will need to be prepared to accept a range of documents.

Statutory requirements (paraphrased wording)

11. *Requirements for identification measures are summarised in Article 3. Among other things, identification measures must establish the persons who are concerned with a legal arrangement, and each beneficial owner and controller of a customer who is a legal person.*

12. *Under Article 3(2)(b) of the Money Laundering Order a relevant person must determine whether a customer is acting for a legal arrangement, and, if so, identify the legal arrangement.*

13. *Where a customer is acting for a legal arrangement, Article 3(2)(a) of the Money Laundering Order requires the customer, e.g., the trustee of a trust or general partner of a limited partnership, to be identified.*

14. *Article 3(2)(b)(iii) of the Money Laundering Order requires the identity of each person who falls within Article 3(7) of the Money Laundering Order to be found out and evidence of identity obtained, i.e.:*

- *in the case of a trust, the settlor;*
- *in the case of a trust, the protector;*
- *having regard to risk, a person that has a beneficial interest in the legal arrangement, or who is the object of a trust power in relation to a trust;*
- *any other individual who otherwise exercises ultimate effective control over the third party.*

15. *In respect of each person falling within Article 3(7) of the Money Laundering Order who is not an individual, Article 3(2)(b)(iii) of the Money Laundering Order requires each individual who is that person's Beneficial owner and/or controller to be identified.*

4.3 Obligation to find out identity and obtain evidence: individuals

Overview

16. The following paragraphs apply to situations where an individual is the *customer* or where the *customer* is more than one individual, such as spouses opening a joint account.

17. The provisions also apply to situations where an individual is:

- a person connected to a legal arrangement, because of a requirement in Article 3(2)(b)(iii) of the *Money Laundering Order* to identify each person who falls within Article 3(7) of the *Money Laundering Order*, and each individual who is that person's *Beneficial owner and/or controller;*
- the *Beneficial owner and/or controller* of a *customer*, because of a requirement in Article 3(2)(c)(iii) of the *Money Laundering Order* to identify the individuals who are the *customer's Beneficial owners and/or controllers;*
- acting on behalf of a *customer* (e.g. is acting according to a power of attorney, or has signing authority over an account) because of a requirement in Article 3(2)(aa) of the *Money Laundering Order;* or
- a third party on whose behalf a *customer* is acting, because of a requirement in Article 3(2)(b)(ii) of the *Money Laundering Order* to identify the individuals who are the third party's *Beneficial owners and/or controllers*.

4.3.1 Finding out identity

Guidance notes

18. A *supervised person* may demonstrate that it has found out the identity of an individual who is a *customer* under Article 3(2)(a) of the *Money Laundering Order* where it collects all the following:

	Finding out identity
Legal name, name(s) currently used, any former legal name(s), and name(s) formerly used	✓
Principal residential address	✓
Date of birth	✓
Place of birth	✓
Nationality	✓
Gender identity	✓
Passport or national identity number	✓

19. However, in the case of a lower risk relationship, a *supervised person* may demonstrate that it has found out the identity of an individual who is a *customer* under Article 3(2)(a) of the *Money Laundering Order* where it collects all the following:

	Finding out identity	**Obtaining evidence**
Legal name, name(s) currently used, any former legal name(s), and name(s) formerly used	✓	✓ **AND** EITHER…
Principal residential address	✓	✓

Date of birth	✓	OR ✓

4.3.2 Obtaining evidence of identity

Overview

20. Evidence of identity may come from several sources, including one or more of the following:

- original documents (see this section of *the Handbook*);
- certified copies of documents (see section 4.2.4 of *this Handbook*);
- external data sources (see section 4.2.5 of *this Handbook*); and/or
- *Digital ID* (see section 4.2.6 of *this Handbook*).

21. These sources may differ in their integrity, reliability, and independence. For example, some identification documents are issued after due diligence on an individual's identity has been undertaken (e.g., passports and national identity cards). Others are issued on request, without any such checks being carried out. Furthermore, some documents are more easily forged than others. Therefore, a *supervised person* will need to ensure that its *CDD systems and controls* incorporate measures specifically designed to do so – see section 4.2.5 of *this Handbook*.

22. Additionally, documents incorporating photographic confirmation of *customer* identity provide a higher level of assurance that an individual is the person they claim to be.

23. Where a *supervised person* is not familiar with the form of evidence obtained, appropriate additional measures may be necessary to become satisfied that the evidence is genuine.

24. Other acceptable methods of obtaining evidence of identity may be possible outside those referenced at paragraph 20 above, provided they are equally as robust in terms of verifying that the person being identified is who they claim to be. Methods which are not equally as robust risk the *supervised person* not being able to demonstrate compliance with the requirements of the *Money Laundering Order*.

25. A *supervised person* should apply a risk-based approach to determine what kind of measures might be appropriate for each person being identified and whether the evidence obtained is reasonably capable of verifying that the person is who they say they are.

26. Whether any particular measure outside those referenced at paragraph 20 above is in compliance with the regulatory requirements will be determined on a case-by-case basis. A *supervised person* will be expected to demonstrate how the measure applied is equally as robust. This may be achieved, for example, by identifying and describing the safeguards or controls incorporated into the measure.

27. Where evidence of identity obtained subsequently expires, e.g., a passport, national identity card, or driving licence, it is not necessary to obtain further evidence under *identification measures* set out in Article 13 of the *Money Laundering Order*. However, a *supervised person* should keep in mind that updated evidence of identity may need to be requested at, for example, a trigger event or an increase in the level of *money laundering/terrorist financing/proliferation financing* risk (see section 6 of *this Handbook* for more detail).

AML/CFT/CPF Codes of Practice

[COP36] All key documents (or parts thereof) obtained as evidence of identity must be understandable (i.e., in a language understood by an employee of the *supervised person*) and must be translated into English at the request of the *FIU* or the *JFSC*.

Guidance notes

28. A supervised person may demonstrate that it has obtained evidence under Article 3(2)(a) of the Money Laundering Order that is reasonably capable of verifying that an individual to be identified is who they are said to be where that evidence covers the following components of identity and, where documentary evidence of identity is exclusively relied upon, uses at least two sources of evidence (see paragraph 30 below):

	Obtaining evidence
Legal name, name(s) currently used, any former legal name(s), and name(s) formerly used	✓
Principal residential address	✓
Date of birth	✓
Place of birth	✓
Nationality	✓
Gender identity	✓
Passport or national identity number	✓

29. However, in the case of a lower risk relationship, a *supervised person* may demonstrate that it has obtained evidence that is reasonably capable of verifying under Article 3(2)(a) of the *Money Laundering Order* that an individual to be identified is who they are said to be where that evidence covers the following components, using at least one source of evidence (see paragraph 30 below):

	Obtaining evidence
Legal name, name(s) currently used, any former legal name(s), and name(s) formerly used	✓ **AND** EITHER…
Principal residential address	✓ **OR**
Date of birth	✓

30. A *supervised person* may demonstrate that it has obtained evidence under Article 3(2)(a) of the *Money Laundering Order* that is reasonably capable of verifying that an individual to be identified is who they are said to be where that evidence is one of the following documents:

All elements of identity

- a current passport or copy of such a passport certified by a suitable certifier - providing photographic evidence of identity;
- a current national identity card or copy of such national identity card certified by a suitable certifier - providing photographic evidence of identity; or
- a current driving licence or copy of such driving licence certified by a suitable certifier - providing photographic evidence of identity - where the licensing authority carries out a check on the holder's identity before issuing.

Residential address

- correspondence from a central or local government department or agency (e.g., Government and Parish authorities);
- a letter of introduction confirming residential address from:
  - a *supervised person* that is regulated by the JFSC;
  - a person carrying on a supervised business which is regulated and operates in a well-regulated country or territory; or
  - a branch or subsidiary of a group headquartered in a well-regulated country or territory which applies group standards to subsidiaries and branches worldwide, and tests the application of and compliance with such standards;
- a bank statement or utility bill; or
- a tenancy contract or agreement.

31. IP address verification and geolocation verification may be leveraged to complement other data sources when authorising the *customer*s residential address. These solutions should not be used in isolation.

32. However, in the case of a lower risk relationship with a *customer* who is resident in Jersey, a *supervised person* may demonstrate that it has obtained evidence under Article 3(2)(a) of the *Money Laundering Order* that is reasonably capable of verifying that an individual to be identified is who they are said to be where that evidence is a:

- Jersey driving licence or
- birth certificate, in conjunction with:
  - a bank statement; or
  - a utility bill; or
  - a document issued by a government source; or
  - a letter of introduction from a *supervised person* that is regulated by the *JFSC*.

33. In circumstances where it would not be possible to take a copy of the evidence of identity, a record may instead be made of the type of document and its number, date and place of issue, so that the document may be obtained from its issuing authority if necessary.

34. A *supervised person* may also demonstrate that it has obtained evidence under Article 3(2)(a) of the *Money Laundering Order* that is reasonably capable of verifying that an individual to be identified is who they are said to be where the data or information comes from an independent data source (see section 4.2.5 of *this Handbook*) or, in the case of a residential address, personal visit to that address.

35. Where an individual’s residential address changes, a *supervised person* may demonstrate that it has obtained evidence under Article 3(2)(a) of the *Money Laundering Order* that is reasonably capable of verifying that an individual to be identified is who they are said to be where the data or information is collected through ongoing correspondence with that *customer* at the changed address.

36. A *supervised person* may demonstrate that a country or territory is well-regulated for the purpose of a letter of introduction, where it has regard to:

- the development and standing of the country or territory's regulatory framework;
- recent independent assessments of its regulatory environment, such as those conducted and published by the *IMF,* the *FATF* and other *FSRBs.*

4.3.2.1 Electronic bank statements and utility bills

Overview

37. It is now common for statements and utility bills to be delivered by e-mail or made available via an online portal (an electronic statement).

38. Common types of electronic statement include, but are not limited to:

- a bank statement bearing the name and residential address of the individual;
- a bill for rates, council tax or utilities bearing the name and residential address of the individual.

Statutory requirements (paraphrased wording)

39. *Article 3(2)(a) of the Money Laundering Order states that identification measures are for identifying the customer.*

40. *Article 3(4)(b) of the Money Laundering Order states that for the purposes of Article 3(2) of the Money Laundering Order, identification of a person includes obtaining evidence, on the basis of documents, data or information from a reliable and independent source, that is reasonably capable of verifying that the person to be identified is who they are said to be and satisfies the person responsible for the identification of a person that the evidence does establish that fact.*

Guidance notes

41. A *supervised person* wishing to accept an electronic statement as evidence of an individual's residential address is required to satisfy itself, through the application of a risk-based approach, that the document presented is sufficient to meet the requirements of Article 3(4)(b) of the *Money Laundering Order*.

42. A *supervised person* is also required to satisfy itself that the acceptance of an electronic statement is commensurate with the risk profile of its *customer.* For example, the use of an electronic statement alone may not be appropriate for a *customer* assessed as higher risk.

43. A *supervised person* should also consider that some types of electronic statement may be more susceptible than others to being stolen, intercepted, tampered with, or otherwise amended, for example, a document sent by e-mail without any encryption.

44. If a *supervised person* becomes concerned regarding the integrity of an electronic statement, for example, if it becomes unsure whether a utility bill has been generated by the named utility company, the *supervised person* should take appropriate additional steps to seek to corroborate the validity of the document. Examples may include:

- the use of an independent data source (see section 4.2.5 of *this Handbook*) to corroborate the address information. This may be achieved by using a third-party database like a credit agency or an electoral roll. The additional corroboration should be sufficient to give the *supervised person* comfort as to the accuracy of the information contained within the electronic statement;

- requesting sight of the delivery mechanism (such as sight of or access to the *customer* portal, details of the document download or e-mail received) to the *customer* from the bank/utility provider, in which the document was attached;
- a telephone call to the provider of the electronic statement which is corroborated by an independent source to verify such provider exists.
- A digital identification system that complies with the FATF Guidance on Digital Identity published on 6 March 2020 as amended or replaced from time to time constitutes a reliable independent source for verification.

45. If it is concluded that an electronic statement is not appropriate, such as in the case of a *supervised person* who is, or becomes, concerned or suspicious of the validity/authenticity of the electronic statement, an alternative form of residential address will need to be obtained.

46. Consideration should be given to whether concerns regarding the integrity of the electronic statement warrant a *SAR*.

47. IP address verification: the IP address can provide a powerful location data point that can assist in proof of address checks. That location information can then be queried against the address provided to determine if there's a match. While an IP address can provide a layer of location data, it's essential to understand that this information is not necessarily 100% accurate. Users might be on an extensive network, which transfers users to a non-local device, or they may be using a VPN, which masks their actual location.

48. Geolocation verification: If using geolocation information from GPS the data is difficult to forge or alter and offers a proximity indication, which is generally precise to within 125 metres. Geolocation can offer a strong signal to understand the precise location. Depending on the use case, this opt-in information helps stop potential fraudsters, or out-of-area applicants from ever becoming a *customer*.

4.3.3 Suitable certification

Overview

49. Suitable certification is a process where, rather than requesting a person to present evidence of identity directly to a *supervised person*, the person is called on to present themselves to a suitable certifier along with original documentation that supports that person's identity (and is current), specifically for the purpose of entering a *business relationship* or *one-off transaction* with a *supervised person*. The effect of this is to create an environment in which *identification measures* in respect of a *customer* (or other person) is applied through a trusted external party and where the *customer* (or other person) is physically present.

50. Suitable certification is not to be confused with a case where a *supervised person* uses Article 16 of the *Money Laundering Order* - which allows reliance to be placed on *reliance identification measures* that have already been completed by an *obliged person* where evidence of identity that may subsequently be provided by that *obliged person* may now be out of date, and where the *obliged person* has a continuing responsibility to the *supervised person* in respect of record-keeping and access to records – in which case section 5 of *this Handbook* is relevant.

51. Nor should the provisions in Sections 4.3.5 and 4.5.7 of *this Handbook* for copy documentation to be provided by a *supervised TCSP* be confused with suitable certification.

Guidance notes

52. For suitable certification to be effective, an individual will need to personally present an original document to an acceptable suitable certifier who is subject to professional rules (or equivalent) providing for the integrity of the certifier's conduct.

53. Acceptable persons to certify evidence of identity (suitable certifiers) may include:

- a member of the judiciary, a senior civil servant, or a serving police or customs officer;
- an officer of an embassy, consulate or high commission of the country of issue of documentary evidence of identity;
- an individual who is a member of a professional body that sets and enforces ethical standards, for example an Advocate or Solicitor;
- an individual that is qualified to undertake certification services under authority of the Certification and International Trade Committee (in Jersey this service is available through the Jersey Chamber of Commerce); or
- a director, officer, or manager of either:
  - a person carrying on a *financial services business* which is regulated and operates in a well-regulated country or territory; or
  - a branch or subsidiary of a group headquartered in a well-regulated country or territory which applies group standards to subsidiaries and branches worldwide and tests the application of and compliance with such standards.

54. In determining whether a country or territory is well-regulated, a *supervised person* may have regard to:

- the development and standing of the country or territory's regulatory framework; and
- recent independent assessments of its regulatory environment, such as those conducted and published by the IMF, the *FATF* and *FSRBs*.

55. Best efforts should be exercised to secure a certified copy of photographic evidence of identity that is of adequate quality, e.g., the photograph is clear, and any text is legible.

56. A higher level of assurance will be provided where the relationship between the certifier and the subject is of a professional rather than personal nature. A person cannot be a suitable certifier if they are:

- related to the person being identified by birth or marriage;
- in a relationship or living with the person being identified.

Guidance notes

57. A suitable certification may take the following forms:

- a hand-written certification which meets the criteria as described in paragraphs 58 and 59 below; or
- an electronic certification which is produced using software as described in paragraph 60 below.

58. A *supervised person* may demonstrate that it has obtained evidence under Article 3(2)(a) of the *Money Laundering Order* that is reasonably capable of verifying that a person to be identified is who they are said to be when it:

› obtains a true copy, signed, and dated by the suitable certifier, of a document that is accompanied by the **confirmation** set out in paragraph 63 below and **adequate information** as set out in paragraph 64 below so that they may be contacted in the event of a query.

59. Applying a risk-based approach – for example where the suitable certifier is connected to a *higher risk country or territory*, based in a different country or territory to that of the person to be identified, or there is reason to believe that certification may not be effective – the *supervised person* should take additional steps in line with paragraph 66 below to validate the credentials of the suitable certifier.

60. **Electronic/digital signature** software is available that locks a certification into a pdf, or a similar file type, which cannot be tampered with. A *supervised person* must be aware of and comfortable with the reliability of the software used. The electronic/digital signature solution must lock the certification into the document for it to be acceptable.

61. Article 9A of the *Electronic Communications Law* provides that a signature, seal, attestation, or notarisation is not to be denied legal effect, validity, or enforceability only because it is in electronic form. Therefore, the certification does not need to be a handwritten signature on a document. It can be an electronic/digital signature which is technologically attached to the document. Article 9C(2) of the *Electronic Communications Law* provides that a person (Person A) may authorise another person to attach Person A's electronic signature to the document on Person A's behalf. It may not, however, simply be an electronic image/photocopy placed on that document (for example a handwritten signature copied onto a document (electronically or physically).

62. In the case of the affixation of an electronic signature to certify a document, we would expect that the suitable certifier is in receipt of the relevant original documentation (as described in 4.2.3 *of this Handbook*) or an electronic statement. The suitable certifier may then produce an electronic copy of such original document and affix their electronic signature in line with the detail provided in paragraphs 58 and 59 above. This would create an electronically certified document.

63. It is not a requirement for a document which has been electronically certified to be received directly from the certifier.

64. The **confirmation** should state that the copy of the document is a true copy of an original document (or extract thereof) that includes information on the identity and/or residential address of an individual.

65. In a case where the document to be certified relates to a legal arrangement or legal person, then the *Guidance notes* in this section apply, except that the documents to be certified will be those that provide evidence of identity of that arrangement or person.

66. An **adequate level of information** to be provided by a suitable certifier will include their name, position or capacity, their address and a telephone number, or email address, at which they can be contacted. This applies regardless of what method of certification is used.

67. The additional steps to be taken to validate the credentials of the suitable certifier may include considering factors such as:

› the stature and track record of the suitable certifier;

› previous experience of accepting certifications from suitable certifiers in that profession or country or territory;

› the adequacy of the framework to counter *money laundering,* the *financing of terrorism,* or the *financing of proliferation* in place in the country or territory in which the suitable certifier is located; and

› the extent to which that framework applies to the suitable certifier.

4.3.3.1 **Certification methods not considered to be suitable certification**

Guidance notes

68. The following methods of certification are not considered to be suitable certification:

- 'certification' of documents where the original document has not been presented to the suitable certifier;
- certification which does not include the **confirmation** set out in paragraph 62 above and **adequate information** as set out in paragraph 64 above;
- certification which includes an image or photograph affixed to a document which is not an electronic signature as described within paragraphs 58 and 59 above;
- production, viewing and screenshotting of documentation during a video call is not an appropriate method of certification due to:
  - the risk of 'deep fake' technology being utilised, whereby the video image and voice of an individual can be manipulated to look and sound like another individual. Biometric and similar matching/checking technology is considered necessary for this risk to be adequately mitigated.

69. The *JFSC* considers that certification by a suitable certifier, in line with the guidance set out at section 4.2.4 of *this Handbook*, provides assurances as to the authenticity of the document which the above-referenced methods are not able to do.

4.3.4 Obtaining evidence of identity – Independent data sources

Overview

70. Independent data sources can provide a wide range of confirmatory material on the identity of a *customer* and can be accessible, for example, through publicly available information (such as registers of electors and telephone directories - to the extent permitted by data protection legislation) and commercially available data sources such as those provided by data services providers, e.g., credit reference agencies and business information service providers.

71. Where a *supervised person* is seeking to obtain reliable and independent evidence of identity using an independent data source, whether by accessing the source directly or by using a data services provider, an understanding of the depth, breadth and quality of the data or information is important in order to determine that the source does in fact provide satisfactory evidence of identity and that the process of obtaining evidence is sufficiently robust to be relied upon.

Guidance notes

72. A *supervised person* may demonstrate that it is satisfied that data or information it has accessed directly from data source(s) is sufficiently extensive, reliable, and accurate under Article 3(2)(a) of the *Money Laundering Order* where:

- the source, scope and quality of the data or information accessed are understood;
- the *supervised person* uses positive data or information source(s) that can be called upon to link a *customer* to both current and historical data and information and
- processes allow the *supervised person* to capture and record the data or information.

73. A *supervised person* may demonstrate that it is satisfied that data or information supplied by a data service provider is sufficiently extensive, reliable, and accurate where:

- it understands the basis of the system used by the data service provider and is satisfied that the system is sufficiently robust, including knowing what checks have been carried out, knowing what the results of these checks were, and being able to determine the level of satisfaction provided by those checks;
- the data services provider is registered with a data protection authority in Jersey, the *EEA*, or a country or territory that has similar data protection provisions to the *EEA*, e.g., Guernsey and the Isle of Man;
- the data services provider either:
  - Accesses:
    - a range of positive data or information sources that can be called upon to link a *customer* to both current and historical data and information;
    - negative data and information sources such as databases relating to fraud and deceased persons;
    - a wide range of alert data sources.
- or otherwise ensures that its source(s) are sufficiently extensive, reliable and accurate;
- processes allow the *supervised person* to capture and record the data or information.

4.3.5 Use of Digital ID

Overview

74. With the ongoing development of remote working and circumstances where *customers* are not physically present, *supervised persons* are increasingly making use of smart phone and tablet applications to capture information, copy documents and take images, liveness checks (including micro streaming) or video recordings of *customers* as part of their *CDD* processes (defined in *this Handbook* as *Digital ID*). This section provides guidance and (where relevant) sets out *AML/CFT/CPF Codes of Practice* in respect of:

- the relevant legal and regulatory obligations in relation to *CDD*;
- the relevant legal and regulatory obligations in relation to new and developing technologies, outsourcing and *customers* who are not physically present;
- risk factors inherently associated with the use of *Digital ID* applications;
- examples of risk mitigants to consider when assessing the potential use of a particular *Digital ID* method or application; and
- examples of practices or methods which are not considered to be *Digital ID*.

75. The FATF has issued Guidance on Digital Identity, March 2020 which *supervised persons* may find useful in developing their own procedures and controls. A digital *identification* system that complies with this guidance, or as amended or replaced from time to time, constitutes a reliable independent source for verification.

76. The guidance in this section may also be relevant in situations where similar processes are undertaken but carried out through means other than smart phone and tablet applications, e.g., the use of self-service kiosks with similar document and image capturing and verification technology.

77. To adequately consider the risks associated with *Digital ID*, the *supervised person's* board/senior management should clearly identify, fully understand, and document what the *Digital ID* application does and does not do. For example:

- is it to be used only to collect information about an individual (finding out identity)?
- is it to be used to obtain evidence of that individual's identity?
- is it to be used to collect more general relationship information about an individual from that individual, e.g., *source of funds*?
- is it to be used to collect information about an individual from reliable and independent data sources? If so, where do these data sources originate, and have they been assessed as to their reliability and/or independence?
- is it to be used for reporting and/or evidence of the checks performed. If so, does this reporting include exceptions or anomalies that require further investigation?

78. Where it is identified that a *Digital ID* application does not cover particular elements of *identification measures* (or more general *CDD* measures) then, in line with Article 13 of the *Money Laundering Order*, those elements should continue to be applied using a *supervised person's* existing *systems and controls* (including *policies and procedures*). For example, a *supervised person* could decide to use a *Digital ID* application to find out and evidence identity, whilst, at the same time, employ a more traditional method to establish and verify a *customer's* address.

79. Where a *supervised person* outsources the collection and verification of evidence of the identity of its clients (the outsourced activity) to a Digital ID service provider, the *supervised person* will need to notify the JFSC under the revised Outsourcing Policy. The submission of an Outsourcing Notification in respect of Digital ID Services will be a straight-through process.

80. **Key components of Digital ID systems**

Identity proofing and enrolment: Who are you? Obtain attributes (name, date of birth, identity number etc) and evidence for those attributes; validate and verify ID evidence and resolve it to a unique identity-proofed person.

Binding: issue credentials/authenticators linking the person in possession/control of the credentials to the identity proofed individual.

Authentication: Are you the identified/verified individual? Establish that the claimant has possession and control of the binding credentials. Authentication applies if the regulated entity conducts identification/verification by confirming the potential *customer*'s possession of pre-existing Digital ID credentials.

FATF Guidance on Digital Identity, 6 March 2020

81. The JFSC is aware that a range of Digital ID applications are commercially available for use by supervised persons. Supervised persons might also make use of Digital ID applications which have been developed in-house or within their wider corporate group. The guidance provided in this section is not intended to express any preference or favour towards any particular method of Digital ID, or any particular Digital ID application. The JFSC does not endorse, nor advise on, specific methods or providers available to supervised persons. It remains the decision of the supervised person whether Digital ID should be utilised in any given circumstance, and/or whether the supervised person will develop its own Digital ID application for these purposes or select a Digital ID application that is commercially available. This choice may be determined, for example, based on the supervised person's customer base and how the supervised person conducts its business.

4.3.5.1 **Legal and regulatory obligations relevant to *Digital ID***

Statutory requirements (paraphrased wording)

82. *Article 3(4) of the Money Laundering Order explains that identification of a person means:*

- ***finding out the identity** of that person, including that person's name and legal status; and*
- ***obtaining evidence** based on documents, data or information from a reliable and independent source, that is reasonably capable of verifying that the person to be identified is who they are said to be and satisfies the person responsible for the identification that the evidence does establish that fact.*

83. *Article 3(4A) of the Money Laundering Order states that for the purposes of Article 3(4)(b) of the Money Laundering Order a digital identification system that complies with the FATF Guidance on Digital Identity published on 6 March 2020 as amended or replaced from time to time constitutes a reliable independent source.*

Overview

84. Using a *Digital ID* application is one way of obtaining evidence of identity. Section 4.2.3 of *this Handbook* explains how a *supervised person* may demonstrate that it has obtained evidence that is reasonably capable of verifying that an individual to be identified is who they are said to be. Among other things, it states that use of the following documentary evidence will be reasonably capable of verifying an individual's identity:

- a current passport, or copy of such a passport certified by a suitable certifier;
- a current national identity card, or copy of such a national identity card certified by a suitable certifier; or
- a current driving licence or copy of such a driving licence certified by a suitable certifier.

85. As an alternative to using documentary evidence, section 4.2.5 of *this Handbook* permits, in certain circumstances, the use of independent data sources to verify that the person to be identified is who they are said to be. In practice, it may be possible to demonstrate compliance with Article 3(4) of the *Money Laundering Order* through a combination of documentary evidence and independent data sources.

86. A *supervised person* may use other tools and/or methods (including *Digital ID* applications) to undertake *CDD* measures, so long as such methods comply with Article 3(4) of the *Money Laundering Order.*

Statutory requirements (paraphrased wording)

87. *Article 11 of the Money Laundering Order requires a relevant person to have policies and procedures for the identification and assessment of risks that arise in relation to the use of new or developing technologies for new or existing products or services.*

88. *Article 15(1)(b) of the Money Laundering Order requires a relevant person to apply enhanced CDD measures when the customer has not been physically present for identification purposes.*

Guidance notes

89. The requirements under Articles 11 and 15(3) of the *Money Laundering Order* and the *AML/CFT/CPF Codes of Practice* set out at section 2.4.4 of *this Handbook* will apply in any circumstances where a part of the *CDD* process is undertaken by an independent third party or *supervised person* via the use of *Digital ID* applications, where the *customer* is not physically present. Accordingly, when deciding whether to make use of a particular *Digital ID* application, a *supervised person* is required to undertake a risk assessment comprising of the following:

- › consider the risks involved in the use of the *Digital ID* application and record the reasons why its use is appropriate;
- › consider the risks involved in outsourcing any part of the *CDD* process to an independent third party using the *Digital ID* application and record the reasons why such outsourcing is appropriate;
- › consider whether the features of the *Digital ID* application effectively mitigate the risks identified;
- › apply any additional measures to ensure that all risks are effectively managed;
- › apply, on a risk-sensitive basis, *enhanced CDD measures* to take account of the particular risks arising due to the fact that the *customer* has not been physically present for identification purposes.

90. A risk assessment as described in the paragraph above is not required to be undertaken by the *supervised person* on each occasion that the particular *Digital ID* application is used, but rather when considering whether to incorporate the use of that *Digital ID* application into its *CDD* measures.

91. When using technology to on-board a *customer* remotely, i.e., when a *customer* is not physically present, and conduct activities by digital or other non-physical present means, for example when interacting via a video call, mail or telephone, it is required that enhanced *CDD* measures be applied.

92. The approval by a *supervised person* of the use of one *Digital ID* application should not be taken to constitute approval of the use of all *Digital ID* applications. It is a requirement that each *Digital ID* application be risk-assessed separately and on its own merits.

93. The *supervised person* is required to ensure that adequate and effective *policies and procedures* are in place to support the use of the *Digital ID* application and are catering for the technology that is being used, as well as for the *supervised person*'s business practices.

94. The *supervised person* is required to ensure appropriate training is in place.

4.3.5.2 **Risks of using Digital *ID***

Overview

95. The use of *Digital ID* applications to apply identification measures presents several inherent risks. Typically, a *Digital ID* application will do one or more of the following:

- › capture information, copy documents and capture an image (e.g., take a photograph) of the *customer* (for instance by way of a camera on a smart phone or tablet);
- › transmit the information, documents or image (either to the *supervised person* or another party);

- compare the information, documents and image captured;
- verify the information or documents against external data sources.

Guidance notes

96. A *supervised person* may demonstrate that it has considered the particular risks that arise when using *Digital ID* applications to copy documents and take photographs for *CDD* purposes when it considers the risks set out below.

97. Risk: Documents are tampered with or forged:

- when original documents are not physically presented, it can be more difficult for a *supervised person* to detect that documents have been tampered with or forged. For example, it may be difficult to detect that another individual's photograph has been fraudulently inserted into a passport when simply viewing an electronic copy of that document;
- similarly, it may be difficult to detect the presence or absence of watermarks or other built-in security features on an identity document when simply viewing an electronic copy of the document.

98. Risk: Captured copies of documents or images are tampered with before or during transmission:

- when an electronic copy of a document or an image has been captured there may be opportunities for the *customer* (or another party) to use software to alter the copy of the document or image before transmitting it. For example, it may be possible for a *customer* to alter details (such as name and date of birth) on the copy of the passport prior to transmission. Similarly, it may be possible to use software to alter the photograph and other biometric data on a copy of an identity document.

99. Risk: Documents presented are stolen or their use unauthorised:

- when a *customer* is not physically presenting identification documents, it is more difficult for a *supervised person* to detect that the documents do not belong to the *customer*. For example, a *customer* may present stolen documentation when using the *Digital ID* application.

100. Risk: External data sources used to verify information are not appropriate/sufficient:

- *Digital ID* applications will often verify the information provided by a *customer* using external data sources. Those data sources may cover a specific geographical region, or a particular type of national identity documentation and may not provide full coverage over a *supervised person's customer* base.

4.3.5.3 **Factors to consider when assessing *Digital ID* applications**

Overview

101. This section lists some potential features of *Digital ID* applications (and wrap-around systems) that may be used to mitigate the risks associated with remote identity verification. Where the *Digital ID* application (or connected system) does not sufficiently mitigate the risk, the *supervised person* will need to ensure that its *CDD systems and controls* (including *policies and procedures*) incorporate measures specifically designed to do so.

102. The features described in the *Guidance notes* below do not represent an exhaustive list. A *supervised person* may consider other features, *systems and controls* (including *policies and procedures*) to be appropriate.

Guidance notes

103. Features of *Digital ID* applications (and wrap-around systems) that may be used to mitigate the risk that documents have been tampered with or forged may include:

- the copy of the document is of a very high level of clarity and resolution, such that its contents can be adequately reviewed without undue difficulty (i.e., the clarity and resolution is still sufficient when zooming in to view a particular element of the document);
- the copy of the document is automatically matched to a pre-defined "template" for the particular form of identity document used;
- the data in the main body of the document is compared to biometric or other data stored in the document's machine-readable zone (MRZ) code;
- data on the document is automatically examined for use of unauthorised print fonts and unexpected character spacing;
- the copy of the document is automatically examined to enable detection of fraudulent documents on the basis of that documents' security features (e.g., watermarks, biographical data, photographs, lamination, UV sensitive ink lines holograms, micro-text, etc.) and the location of various elements in the document (i.e. optical character recognition);
- the copy of the document is examined by individuals specifically trained to detect tampering/forgery (e.g., ex-border agents), or the *Digital ID* application has been designed with the characteristics of this training/expertise in mind.

104. Features of *Digital ID* applications (and wrap-around systems) that may be used to mitigate the risk that a copy of a document or photograph has been tampered with or forged before or during transmission may include:

- the *Digital ID* application itself controls the process of copying the document, taking photographs and transmitting the same, allowing no opportunity to tamper with or manipulate documents or photographs. This is in contrast with, for example, a prospective *customer* taking a photograph of a document and transmitting the PDF file by e-mail, which presents multiple opportunities for interference;
- a highly secure connection is used to transmit copies of documents and photographs;
- the *Digital ID* application's security is regularly tested to guard against hacking or other security breaches.

105. Features of *Digital ID* applications (and wrap-around systems) that may be used to mitigate the risk that documents presented are stolen (or their use unauthorised) may include:

- a "selfie" photograph of the *customer* is taken **and** biometrically compared/matched to the photograph on the identity document presented, in order to verify that they relate to the same individual;
- a video or a "micro-stream" of photographs is taken to identify facial movements, which may help to confirm that the *customer* is present at the time that the video/stream of photographs is taken. Use of anti-impersonation measures such as requiring the user to verbally repeat a word or phrase as dictated by the *supervised person* during a video or

"micro-stream". This may also help to prevent the use of a video/stream of photographs which may have been stolen or use of which is unauthorised;

› a code or password is sent to the *customer* who, immediately before the application of Digital *ID*, is photographed while displaying the code or password - to confirm that the *customer* is present at the time that the photograph is taken to avoid a photograph being taken of a photograph which may have been stolen or use of which is unauthorised;

› use of location matching, where the *Digital ID* application determines that information and copies of documents are captured, and photographs taken at a location that is consistent with the *customer's* place (or country) of residence;

› the requirement that any image taken is adequately illuminated when using the *Digital ID* solution.

4.3.5.4 Record-keeping requirements relevant to the use of *Digital ID*

Guidance notes

106. Where a *supervised person* uses *Digital ID* applications to capture information, copy documents and take photographs of *customer*s as part of their *CDD* processes, adequate records are required to be kept in line with the record-keeping requirements set out in Part 4 of the *Money Laundering Order.*

107. Detailed *AML/CFT/CPF Codes of Practice and Guidance notes* are provided at section 11 of *this Handbook* regarding the requirements of Part 4 of the *Money Laundering Order*.

› Often *Digital ID* systems will allow for *supervised persons* to meet these obligations by (1) providing them with access, on an ongoing basis, to the system which has verified a *customer* or (2) allowing them to download or integrate the documentary evidence which has verified a *customer* to or within their own systems. In either case, *supervised persons* should be confident that the evidence obtained from the *Digital ID* system sets out:

  - details of the biometric checking undertaken;
  - details of what third party data sources have been utilised to verify the *customer* (if any); and
  - details of the audit trail, sign-off or additional steps which have been undertaken commensurate with the risk profile of the *customer*.

4.3.5.5 Practices or methods not considered to be *Digital ID*

Overview

108. Whilst there are a range of *Digital ID* applications which incorporate features that the *JFSC* considers may allow a *supervised person* to comply with Article 3(4) of the *Money Laundering Order*, some other practices or methods are not currently deemed to sufficiently address the risks listed at section 4.3.5.2 of *this Handbook* and are therefore not considered to be *Digital ID*. Examples of these are set out in the *Guidance notes* below.

109. Biometric and similar matching/checking technology is referred to in the *Guidance notes* below. The *FATF* describes biometrics as an individual's personal biological or behavioural characteristics. *Digital ID* applications may make use of the following biometrics as part of their verification processes:

› biophysical biometrics: attributes, such as fingerprints, iris patterns, voiceprints and facial recognition;

- biomechanical biometrics: attributes, such as keystroke mechanics, are the product of unique interactions of an individual's muscles, skeletal system, and nervous system;
- behavioural biometric patterns: attributes, based on the new computational social science discipline of social physics, consist of an individual's various patterns of movement and usage in geospatial temporal data streams, and include, for example, an individual's email or text message patterns, file access log, mobile phone usage, and geolocation patterns.

Guidance notes

110. Use of video calls where an identity document is produced during the call for comparison, but no biometric or similar matching/checking technology is employed, e.g., the *customer* just holds up their passport during a video call – this method is not considered to be appropriate due to:

- there being no independent authentication process alongside the identification document being produced, hence the process is not adequately robust;
- the risk of 'deep fake' technology being utilised, whereby the video image and voice of an individual can be manipulated to look and sound like another individual. Again, biometric and similar matching/checking technology is considered necessary for this risk to be adequately mitigated.

  Whilst a *supervised person* may wish to hold a video call to meet a potential *customer* and discuss elements of the proposed *business relationship* (including **finding out identity** or other *customer* information), that video call is not sufficient for the purposes of obtaining **evidence of identity**. A *Digital ID* application, or other alternative method, may be used for that purpose, enabling the independent authentication process.

111. Using scanned copies of documents (i.e., re-productions of original documents which have not been suitably certified) as evidence of identity – this method is not considered to be appropriate due to:

- the risk that an identity document has been tampered with or forged not being mitigated using specialist checks. The scanned copies in this case are in effect non-certified and non-authenticated. If scanned copies are to be used as evidence, they should be independently verified/authenticated. That verification process may include, for example, the use of third-party data sources or the use of a *Digital ID* application in instances when such technology utilises automated verification technology in a robust and appropriate way. It may, for example, verify data embedded in the scanned document (barcodes, micro-lettering etc.).

112. Using a "selfie" photograph of the *customer* **without** it being biometrically compared/matched to the photograph on the identity document presented to verify that they relate to the same individual, e.g., the *customer* just takes a "selfie" photograph of themselves holding up their passport – this method is not considered to be appropriate due to:

- the risk that an identity document has been tampered with or forged not being mitigated using specialist checks.

  If, however, such a "selfie" photograph is being uploaded to a *Digital ID* application which then undertakes authenticity checks to verify identity, for example by extracting machine-readable text or hologram data, and verifying the data in an appropriate, independent way to ensure it is robust, then this is an acceptable method to evidence identity.

4.3.6 Guarding against the financial exclusion of Jersey residents

Overview

113. On occasions, an individual may be unable to provide evidence of identity using the sources set out at section 4.2.3 of *this Handbook*. Examples of such individuals may include:

- seasonal workers whose principal residential address is not in Jersey;
- individuals living in Jersey in accommodation provided by their employer, with family, or in care homes, who may not pay directly for utility services;
- Jersey students living in university, college, school, or shared accommodation, who may not pay directly for utility services;
- minors.

AML/CFT/CPF Codes of Practice

[COP37] A *supervised person* must determine that there is a valid reason for a *customer* being unable to provide more usual sources of evidence of identity and must document that reason.

Guidance notes

114. In the case of a lower risk minor, whose parent or guardian is unable to produce more usual evidence of identity for the minor, and who would otherwise be excluded from accessing financial services, a *supervised person* may demonstrate that it has obtained evidence under Article 3(2)(a) of the *Money Laundering Order* that is reasonably capable of verifying that a person to be identified is who they are said to be where that evidence is:

- the minor's birth certificate;
- a letter from the parent or guardian confirming their status (i.e., "I am the parent or guardian of [name of minor]") and the residential address of the minor.

115. In the case of a lower risk individual who is resident in a Jersey nursing home or residential home for the elderly and has a valid reason for being unable to produce more usual evidence of identity, and would otherwise be excluded from accessing financial services, a *supervised person* may demonstrate that it has obtained evidence under Article 3(2)(a) of the *Money Laundering Order* that is reasonably capable of verifying that a person to be identified is who they are said to be where that evidence is a letter from a Jersey nursing home or residential home for the elderly, which a *supervised person* is satisfied that it can place reliance on, confirming the identity of the resident.

116. In other cases, where a lower risk individual has a valid reason for being unable to produce more usual evidence of identity, and would otherwise be excluded from accessing financial services, a *supervised person* may demonstrate that it has obtained evidence under Article 3(2)(a) of the *Money Laundering Order* of residential address that is reasonably capable of verifying that a person to be identified is who they are said to be where that evidence is a letter from:

- a Jersey employer, which a *supervised person* is satisfied that it can place reliance on, that confirms residence of an individual at a stated Jersey address, and, in the case of a seasonal worker, indicates the expected duration of employment and gives the worker's principal residential address in their country of origin;
- the head of household at which the individual resides confirming that the individual lives at that Jersey address, setting out the relationship between the *customer* and the head of household, together with evidence that the head of household resides at the address; or
- a principal of a university or college, which a *supervised person* is satisfied that it can place reliance on, that confirms residence of the individual at a stated address. In the case of a

Jersey student studying outside the Island, a residential address in Jersey should also be collected.

117. Confirmatory letters should be written on appropriately headed paper.

4.3.7 Residential address: Overseas residents

Overview

118. On occasions, an individual that resides abroad may be unable to provide evidence of their principal residential address using the sources set out at section 4.2.3 of *this Handbook.* Examples include residents of countries without postal deliveries and few street addresses, who rely upon post office boxes or employers for delivery of mail, and residents of countries where, due to social restraints, evidence of a private address may not be obtained through a personal visit.

119. It is essential for law enforcement purposes that a record of an individual's residential address (or details of how that individual's place of residence may be reached) be recorded. As a result, it is not acceptable to only record a post office box number as an address.

AML/CFT/CPF Codes of Practice

[COP38] A *supervised person* must determine that there is a valid reason for a *customer* being unable to provide more usual sources of evidence for an address and must document that reason.

[COP39] Where alternative methods to obtain evidence for an address are relied on, a *supervised person* must consider whether enhanced monitoring of activity and transactions is appropriate.

Guidance notes

120. Where an individual has a valid reason for being unable to produce more usual evidence for a residential address, a *supervised person* may demonstrate that it has obtained evidence under Article 3(2)(a) of the *Money Laundering Order* that is reasonably capable of verifying that a person to be identified is who they are said to be where it receives written confirmation from an individual satisfying the criteria for a suitable certifier that they have visited the individual at that address.

121. Where an individual has a valid reason for being unable to produce more usual evidence for a residential address, a *supervised person* may demonstrate that it has found out the identity of that person under Article 3(2)(a) of the *Money Laundering Order* where, in addition to principal residential address, it collects a "locator address." In such a case, a *supervised person* may demonstrate that it has obtained evidence that is reasonably capable of verifying that a person to be identified is who they are said to be where it obtains evidence that the individual may normally be met or contacted at that address.

122. A "locator address" is an address at which it would normally be possible to physically meet or contact an individual (with or without prior arrangement), for example, an individual's place of work.

4.4 Obligation to find out identity and obtain evidence: Legal arrangements

Overview

123. Jersey law recognises two distinct forms of legal arrangement: the trust and the limited partnership.

124. Jersey trusts law comprises both the *Trust Law*, as amended, and the Jersey customary law of trusts. Limited partnerships are established under the Limited Partnerships (Jersey) Law 1994. Limited Liability Partnerships, Separate Limited Partnerships and Incorporated Limited Partnerships all have legal personality and are therefore covered in section 4.4 of *this Handbook.*

125. There are a wide variety of trusts ranging from large, nationally, and internationally active organisations subject to a high degree of public scrutiny and transparency, through to trusts set up under testamentary arrangements or established for wealth management purposes. Trusts may also be established as *Collective investment scheme*s – known as unit trusts.

126. A legal arrangement cannot form a *business relationship* or carry out a *one-off transaction* itself. It is the trustee(s) of the trust or general partner(s) of the limited partnership who will enter a *business relationship* or carry out the *one-off transaction* with a *supervised person* on behalf of the legal arrangement and who will be the *customer*(s). In line with Article 3 of the *Money Laundering Order*, the trust or limited partnership will be the third party on whose behalf the trustee(s) or general partner(s) act(s).

127. In forming a *business relationship* or carrying out a *one-off transaction* with a trustee or general partner, a *supervised person* will be dependent on information provided by the trustee or general partner (a supervised Trust Company Business or otherwise) relating to the legal arrangement and persons concerned with the legal arrangement (set out in Article 3(7) of the *Money Laundering Order*). When determining the risk assessment for a legal arrangement (section 3.3 of *this Handbook*), the risk factors set out in section 3.3.4.1 and sections 8.1.2 and 8.2.1 of *this Handbook* will be relevant in deciding whether it is appropriate to use information provided by the trustee or general partner. In addition, the monitoring measures maintained by a *supervised person* (see section 6 of *this Handbook*) may provide additional comfort that relevant and up-to-date information on identity has been found out.

128. In the case of a unit trust which is a third party, individual investors into the unit trust are not considered to be settlors for the purpose of Article 3(7)(a) of the *Money Laundering Order*. However, the investors may in certain circumstances be considered *Beneficial owners and/or controllers* and are *customers* of the fund (see section 12 of *this Handbook*).

129. The following provisions apply to situations where a trustee of an *express trust* or general partner of a limited partnership is the *customer* of a *supervised person*. Sector-specific sections for Trust Company Business and funds and fund operators explain the *identification measures* to be applied by a trustee or general partner itself in respect of the legal arrangement. See sections 12 and 13 of *this Handbook*.

130. The provisions will also assist with the identification of ultimate *Beneficial owners and/or controllers* and will be relevant in situations where a legal arrangement (through the trustee or general partner) is:

› the *owner or controller* of a *customer*, because of a requirement in Article 3(2)(c)(iii) of the *Money Laundering Order* to identify the individuals who are the *customer's Beneficial owners and/or controllers*; or

› a third party on whose behalf a *customer* is acting, because of a requirement in Article 3(2)(b)(ii) of the *Money Laundering Order* to identify the individuals who are the third party's *Beneficial owners and/or controllers*.

131. Where the trustee or general partner is a *supervised person* carrying on *regulated business* or is a person who carries on *equivalent business* to any category of *regulated business*, it may be possible to apply *CDD* exemptions under Article 17B and Article 18(3) of the *Money Laundering Order*. See section 8 of *this Handbook*.

132. The measures that must be applied by a *supervised person* where a third party is a trust need not include a settlor of a trust who is deceased.

133. The measures that must be applied to obtain evidence of identity of **beneficiaries** and persons **who are the object of a power** and have been identified as **presenting higher risk** will necessarily reflect the verification methods that are available at a particular time to the trustee. For example, it may not be appropriate to request evidence directly from the beneficiary or object of a power.

134. Where a *supervised person* is not familiar with the form of evidence of identity obtained to verify identity, appropriate measures may be necessary to satisfy itself that the evidence is genuine.

135. Notwithstanding the requirement to find out identity and obtain evidence of identity in relation to the trustee, the trust and those individuals listed in Article 3(7) of the *Money Laundering Order*, a *supervised person* is not expected to collect information on the detailed terms of the trust, nor rights of the beneficiaries.

4.4.1 Finding out identity – Legal arrangement that is a trust

Guidance notes

136. A *supervised person* may demonstrate that it has found out the identity of a trust which is a third party under Article 3(2)(b)(i) of the *Money Laundering Order* where it collects all the following components of identity:

- name of trust;
- date of establishment;
- official identification number (e.g., tax number or registered charity or non-profit organisation number); and
- mailing address of trustee(s).

137. A *supervised person* may demonstrate that it has found out the identity of the settlor of a trust which is a third party under Article 3(2)(b)(iii)(B) of the *Money Laundering Order* where it finds out the identity of:

- the settlor (including any persons subsequently settling funds into the trust);
- any person who directly or indirectly provides trust property or makes a testamentary disposition on trust or to the trust; and
- any other person exercising **ultimate effective control** over the trust, for example, a protector.

138. This information may be provided by the trustee.

139. A *supervised person* may demonstrate that it has found out the identity of persons having a beneficial interest in a trust (other than a unit trust) which is a third party under Article 3(2)(b)(iii)(B) of the *Money Laundering Order* where it finds out the identity of each beneficiary with a vested right. This information may be provided by the trustee.

140. A *supervised person* may demonstrate that it has found out the identity of persons having a beneficial interest in a trust (other than a unit trust) which is a third party under Article 3(2)(b)(iii)(B) of the *Money Laundering Order* where it finds out the identity of each beneficiary who has been identified as presenting higher risk. This information may be provided by the trustee.

141. A *supervised person* may demonstrate that it has found out the identity of persons having a beneficial interest in a unit trust (for example a Jersey Private Fund) which is a third party under Article 3(2)(b)(iii)(B) of the *Money Laundering Order* where, having regard to risk, it finds out the identity of investors holding a material interest in the capital of the unit trust. This information may be provided by the trustee.

142. A *supervised person* may demonstrate that it has found out the identity of persons who are the object of a trust power in a trust which is a third party under Article 3(2)(b)(iii)(B) of the *Money Laundering Order* where it finds out the identity of each person who is the object of a power and has been identified as presenting higher risk. This information may be provided by the trustee.

143. A *supervised person* may demonstrate that it has found out the identity of any other person who otherwise exercises ultimate effective control over the third party under Article 3(2)(b)(iii)(B) of the *Money Laundering Order* where it finds out the identity of each co-trustee. This information may be provided by the trustee.

144. In any case where a settlor, protector, beneficiary, object of a power, or other person referred to in paragraphs 129 to 135 above (the "person") is not an individual, a *supervised person* may demonstrate that it has identified everyone who is the person's *Beneficial owner and/or controller* under Article 3(2)(b)(iii)(C) of the *Money Laundering Order* where it has identified:

i. **each** individual with a **material controlling ownership interest** in the capital of the person (through direct or indirect holdings of interests or voting rights) or who exerts **control through other ownership means;**

ii. **to** the extent that there is doubt as to whether the individuals exercising control through ownership are *Beneficial owners*, or where no individual exerts control through ownership, any other individual exercising **control** over the person **through other means.** This effectively means that anyone exercising control through ownership and anyone exercising control through other means must be ascertained;

iii. where no individual is otherwise identified under sub-paragraphs (i) and (ii) above, individuals who exercise **control** of the person **through positions held** (e.g., those who have and exercise strategic decision-taking powers or have and exercise executive control through senior management positions).

Refer to the flow-chart at section 4.5.1 *of this Handbook* for a graphical explanation of the process described in the paragraph above.

145. For lower risk relationships, a general threshold of 25% is considered to indicate a material controlling ownership interest in capital. Where the distribution of interests is uneven, the percentage where effective control may be exercised (a material interest) may be less than 25% when the distribution of other interests is considered, i.e., interests of less than 25% may be material interests.

4.4.2 Obtaining evidence of identity – Legal arrangement that is a trust

AML/CFT/CPF Codes of Practice

[COP40] All key documents (or parts thereof) obtained as evidence of identity must be understandable (i.e., in a language understood by an employee of the *supervised person*) and must be translated into English at the request of the *FIU* or the *JFSC*.

[COP41] A *supervised person* must obtain evidence that any person purporting to act as the trustee of a trust which is a third party has authority to act in such capacity.

Guidance notes

146. A *supervised person* may demonstrate that it has obtained evidence under Article 3(2)(b)(i) of the *Money Laundering Order* that is reasonably capable of verifying that a trust which is a third party to be identified is what it is said to be where the evidence covers the following components of identity:

- name of trust;
- date of establishment;
- date of appointment of the trustee;
- nature of the trustee's powers.

This need not involve a review of an existing trust instrument (or similar instrument) as a whole – reviewing or obtaining copies of relevant extracts of a trust instrument may suffice.

4.4.3 Finding out identity – Legal arrangement that is a limited partnership

Guidance notes

147. A *supervised person* may demonstrate that it has found out the identity of a limited partnership which is a third party under Article 3(2)(b)(i) of the *Money Laundering Order* where it collects all the following:

- name of partnership;
- any trading names;
- date and country/territory of registration/establishment;
- official identification number;
- registered office/business address;
- mailing address (if different);
- principal place of business/operations (if different); and
- names of all general partners and those limited partners that participate in management (if any).

148. A *supervised person* may demonstrate that it has found out the identity of a person who has a **beneficial interest** in a limited partnership which is a third party under Article 3(2)(b)(iii)(B) of the *Money Laundering Order* where it finds out the identity of limited partners holding a **material controlling ownership interest** in the capital of the partnership (through direct or indirect holdings of interests or voting rights) or any other person **exercising control through other ownership means**, e.g. partnership agreements, power to appoint senior management, or any outstanding debt that is convertible into voting rights.

149. To the extent that there is doubt as to whether the persons exercising control through ownership are *beneficial owners*, or where no person exerts control through ownership, a *supervised person* may demonstrate that it has found out the identity of a person who has a **beneficial interest** in a limited partnership which is a third party under Article 3(2)(b)(iii)(B) of the *Money Laundering Order* where it finds out the identity of those who exercise **control through other means**, e.g., those who exert control through personal connections, by participating in financing, because of close family relationships, historical or contractual associations or as a result of default on certain payments.

150. Where no person is otherwise identified under this section, a *supervised person* may demonstrate that it has found out the identity of a person who has a **beneficial interest** in a limited partnership which is a third party under Article 3(2)(b)(iii)(B) of the *Money Laundering Order* where it finds out the identity of persons who **exercise control through positions held** (e.g., those who have and exercise strategic decision-making powers or have and exercise executive control through senior management positions, e.g., general partner or limited partner that participates in management). This information may be provided by the general partner.

151. In any case where a partner (including a general partner) or other person referred to in paragraphs 140 to 142 above is not an individual, a *supervised person* may demonstrate that it has identified each individual who is that person's *Beneficial owner and/or controller* under Article 3(2)(b)(iii)(C) of the *Money Laundering Order* where it has identified:

i. each individual with a material controlling ownership interest in the capital of the partnership (through direct or indirect holdings of interests or voting rights) or who exerts control of the partnership through other ownership means;

ii. to the extent that there is doubt as to whether the individuals exercising control through ownership are beneficial owners, or where no individual exerts control through ownership, any other individual exercising control over the partnership through other means. This effectively means anyone exercising control through ownership and anyone exercising control through other means must be ascertained;

iii. where no individual is otherwise identified under sub-paragraphs (i) and (ii), individuals who exercise control of the partnership through positions held (e.g., those who have and exercise strategic decision-taking powers or have and exercise executive control through senior management positions).

Refer to the flow-chart at section 4.5.1 of *this Handbook* for a graphical explanation of the process described in the paragraph above.

152. In the case of a lower risk relationship, partners who have and exercise authority to operate a *business relationship* or *one-off transaction* will be individuals who exercise control through positions held.

153. For lower risk relationships, a general threshold of 25% is considered to indicate a material controlling ownership interest in the capital of a limited partnership. Where the distribution of interests is uneven the percentage where effective control may be exercised (a material interest) may be less than 25% when the distribution of other interests is considered, i.e., interests of less than 25% may be material interests.

4.4.4 Obtaining evidence of identity – Legal arrangement that is a limited partnership

AML/CFT/CPF Codes of Practice

[COP42] All key documents (or parts thereof) obtained as evidence of identity must be understandable (i.e., in a language understood by an employee of the *supervised person*) and must be translated into English at the request of the *FIU* or the *JFSC.*

[COP43] A *supervised person* must obtain evidence that any person purporting to act as general partner of a partnership which is a third party has authority to act in such capacity.

Guidance notes

154. A *supervised person* may demonstrate that it has obtained evidence under Article 3(2)(b)(i) of the *Money Laundering Order* that is reasonably capable of verifying that a limited partnership which is a third party to be identified is what it is said to be where the evidence covers all of the following components of identity:

- name of partnership;
- date and country/territory of registration/establishment;
- official identification number;
- registered office/business address; and
- principal place of business/operations (if different).

155. However, in the case of a lower risk relationship, a *supervised person* may demonstrate that it has obtained evidence under Article 3(2)(b)(i) of the *Money Laundering Order* that is reasonably capable of verifying that a limited partnership which is a third party to be identified is what it is said to be where the evidence covers the following components of identity:

- name of partnership;
- date and country/territory of registration/establishment;
- official identification number.

156. A *supervised person* may demonstrate that it has obtained evidence under Article 3(2)(b)(i) of the *Money Laundering Order* that is reasonably capable of verifying that a limited partnership which is a third party to be identified is what it is said to be where it obtains, in every case, the partnership agreement or a copy of such an agreement certified by a suitable certifier and one or more sources of further evidence (one source for lower risk *customer*s):

- certificate of registration (where a partnership is registered) or copy of such a certificate certified by a suitable certifier;
- latest audited financial statements or a copy of such statements certified by a suitable certifier.

157. A *supervised person* may also demonstrate that it has obtained evidence under Article 3(2)(b)(i) of the *Money Laundering Order* that is reasonably capable of verifying that a partnership which is a third party is what it is said to be where the data or information comes from an independent data source (see *Guidance notes* at section 4.3.4 of *this Handbook*) or (in the case of a principal place of business) personal visit to that address. An independent data source may include a registry search, which confirms that the partnership is not in the process of being dissolved, struck off, wound up or terminated.

158. Where a partner holds their role by virtue of their employment by (or position in) a business that is a supervised Jersey *TCSP*, a *supervised person* may demonstrate that it has taken reasonable measures to find out the identity of that person and to obtain evidence under Article 3(2)(b)(iii)(B) of the *Money Laundering Order* where it obtains the following:

- the full name of the partner;
- an assurance from the *TCSP* that the individual is an officer or employee.

4.4.5 Copy documentation provided by *CD regulated TCSP*

Guidance notes

159. Where information is provided by a *TCSP* that is regulated by the *JFSC*, the Guernsey Financial Services Commission or the Isle of Man Financial Services Authority, a CD regulated TCSP, on a person listed in Article 3(7) of the *Money Laundering Order* (following an assessment of risk in line with paragraph 119 above, or paragraph 174 below), a *supervised person* may demonstrate that it has taken reasonable measures to obtain evidence of identity for that person under Article 13 of the *Money Laundering Order* where it obtains a copy of a document that is listed in paragraph 31 from the *CD regulated TCSP*, along with the confirmations set out in the paragraph below.

160. The confirmations to be obtained are that:

› the *CD regulated TCSP* has seen the original document that it has copied to the *supervised person*, or the document that has been copied to the *supervised person* was provided to the *CD regulated TCSP* by a suitable certifier, or the evidential report copied to the *supervised person* has been obtained by the *CD regulated TCSP* as a result of utilising a *Digital ID* system which meets the requirements of *this Handbook*;

› the *CD regulated TCSP* is satisfied that the original document seen, or document provided to it by a suitable certifier, or documentary evidence permissible within a *Digital ID* system, provides evidence that the individual is who they are said to be; and

› the document provided to the *supervised person* is a true copy of a document (or evidential report) that is held by the *CD regulated TCSP*.

161. This will be different to a case where a *supervised person* decides to make use of Article 16 of the *Money Laundering Order* - which allows reliance to be placed on *reliance identification measures* that have already been completed by an *obliged person* where evidence of identity may be held by the *obliged person*, and where the *obliged person* has a continuing responsibility to the *supervised person* in respect of record-keeping and access to records - see section 5 of *this Handbook.*

162. In both cases, the risk of placing reliance on another person to have carried out *identification measures* must be considered – either as part of an assessment of *customer* risk under Article 13 of the *Money Laundering Order*, or assessment of risk under Article 16 of the *Money Laundering Order.*

163. Nor should provision for copy documentation to be provided by a *CD regulated TCSP* be confused with “suitable certification”, which is explained in section 4.3.3 of *this Handbook*.

164. For the avoidance of doubt this is a very limited provision applying to *regulated TCSP* and does not extend to other types of *supervised business*.

4.4.6 Identification measures – Unit trusts

Guidance notes

165. A unit trust is defined in the Trusts Law as “…any trust established for the purpose, or having the effect, of providing, for persons having funds available for investment, facilities for the participation by them as beneficiaries under the trust, in any profits or income arising from the acquisition, holding, management or disposal of any property whatsoever”.

166. Unit trusts are therefore primarily for investment and differ in structure from the more traditional discretionary trust. A unit trust may be established for different purposes, some examples of why it may be established include:

› by someone who wishes to use it as an investment vehicle for themselves and others but wishes to share the costs as well as the profits;

› by an investment manager or investment bank to offer an investment opportunity to its *customers*;

› as a holding vehicle for property or other assets.

167. The settlor of a trust is defined in the *Trust Law* as "… a person who provides trust property or makes a testamentary disposition on trust or to a trust". Consideration should be given as to whether a promoter/instigator/arranger is the settlor, i.e., whether they contribute property to the unit trust directly or indirectly. Where the promoter/instigator/arranger is not a settlor the *supervised person* should find out who they are to be able to adequately assess the risk of the relationship with the *customer*, being the trustee of the unit trust.

168. While the individual investors are not considered to be settlors for the purposes of Article 3(7)(a) of the *Money Laundering Order* (see section 13.3.3 of *this Handbook*), each of the unit holders will be *customers* of the trustee (who is acting on behalf of the unit trust), investing their money into the unit trust. This may include the promoter/instigator/arranger as an investor. In the *Trust Law* a unit holders' entitlement is described as "participation by them as beneficiaries under the trust."

169. The trustee of the unit trust is required to maintain adequate, accurate and current basic and beneficial ownership information in relation to the unit trust (see section 12.2.4.1 of *this Handbook*). The trustee will apply *identification measures* to each of the unit holders (the trustee's *customers*) based on the structure of that unit holder, whether they be individuals, legal persons, or legal arrangements (see section 4 and section12.2.4.1 of *this Handbook*).

170. Where a *supervised person* forms a *business relationship* with the trustee(s) who are acting for the benefit of the unit trust they should apply *identification measures* to:

› The settlor (see paragraph 167 above) and (if any) the protector;

› The trustee (there may be more than one) who is the *Governing body* of the unit trust and contracts on its behalf and is the "*customer*";

› Any third parties on whose behalf the trustee(s) are acting. When dealing with a unit trust, a *supervised person* may demonstrate compliance with Article 3(7) (b) (i) of the *Money Laundering Order* where they apply *identification measures* to those unit holders who exercise control over the unit trust or who are deemed to have a material controlling interest of 25% (in lower risk scenarios). In higher risks scenarios, unit holders holding interests of less than 25% may need to be identified and verified. Even where unit holders are not identified and verified (as they fall below the thresholds) sufficient information will need to be obtained about the unit holders to know who they are for the purposes of the risk assessment, *customer* profiles (see section 13.2.5 of *this Handbook*) may be used; and

› any other parties who exercise ultimate control over the trust, such as by other means – for example where an investment manager is the instigator of the unit trust and manages the investments of the unit trust.

171. Good practice would be to ensure the terms of engagement/business with the trustee(s) require notification of changes to the *beneficial ownership* and *control structure* and any other events that may impact on the risk of the *customer* relationship.

4.5 Obligation to find out identity and obtain evidence: Legal Persons

Overview

172. Jersey law recognises several distinct forms of legal person, in particular:

- companies, established under the *Companies Law*;
- foundations, established under the *Foundations Law*;
- limited liability partnerships, established under the Limited Liability Partnerships (Jersey) Law 2017;
- separate limited partnerships, established under the Separate Limited Partnerships (Jersey) Law 2011;
- incorporated limited partnerships, established under the Incorporated Limited Partnerships (Jersey) Law 2011;
- limited liability companies, established under the Limited Liability Companies (Jersey) Law 2018.

173. The following provisions apply to situations where a legal person is the *customer*.

174. The provisions will also assist with the identification of ultimate *Beneficial owners and/or controllers* and will be relevant in situations where a legal person is:

- a person connected to a legal arrangement, because of a requirement in Article 3(2)(b)(iii) of the *Money Laundering Order* to identify each person who falls within Article 3(7) of the *Money Laundering Order*, and each individual who is that person's *Beneficial owner and/or controller*;
- the owner or controller of a *customer*, because of a requirement in Article 3(2)(c)(iii) of the *Money Laundering Order* to identify the individuals who are the *customer's Beneficial owners and/or controllers*;
- acting on behalf of a *customer* (e.g., is acting according to a power of attorney, or has signing authority over an account);
- a third party on whose behalf a *customer* is acting, because of a requirement in Article 3(2)(b)(ii) of the *Money Laundering Order* to identify the individuals who are the third party's *Beneficial owners and/or controllers*.

175. The *Companies Law* allows for the incorporation of cell companies: *ICCs* and *PCCs*. Each of these types of cell companies may establish one or more cells.

176. In the case of a *PCC*, each cell, despite having its own memorandum of association, shareholders, and directors, as well as being treated for the purposes of the *Companies Law* as if it were a company, does not have a legal personality separate from the cell company. Accordingly, where a cell wishes to contract with another party, it does so through the cell company acting on its behalf. To ensure that creditors and third parties are aware of this position, a director of the cell company is under a duty to notify the counterparties to a transaction that the cell company is acting in respect of a particular cell.

177. Where a *supervised person* establishes a *business relationship* or enters into a *one-off transaction* with a cell of a *PCC*, because the cell does not have the ability to enter into arrangements or contract in its own name, for the purposes of Article 3 of the *Money Laundering Order*, the *PCC* will be taken to be a *customer* acting for a third party and the particular cell will be taken to be the third party that is a person other than an individual.

178. By contrast, in the case of an *ICC,* each cell has its own separate legal personality, with the ability to enter into arrangements or contracts and to hold assets and liabilities in its own name. Where a *supervised person* establishes a *business relationship* or enters into a *one-off transaction* with a cell of an *ICC*, the cell will be taken to be the *customer.*

179. In a case where the ownership structure of a legal person to be identified (Legal Person A) includes other legal persons, the beneficial owners and controllers of Legal Person A will include those individuals **ultimately** holding a **material controlling ownership** interest in Legal Person A.

180. The *identification measures* to be applied to each type of person are set out in *this Handbook* as follows:

› a company: sections 4.5.1 and 4.5.2;

› a foundation: sections 4.5.3 and 4.5.4;

› a partnership: sections 4.5.5 and 4.5.6.

181. For the purpose of this section, provisions that are said to apply to a company are to be taken to apply, with appropriate modification, to:

› any other body that can establish a *business relationship* with a *supervised person* or otherwise own property;

› an anstalt;

› an incorporated or unincorporated association, club, society, charity, church body, or institute;

› a mutual or friendly society;

› a co-operative;

› a provident society.

182. Where information relating to a legal person is not available from a public source, a *supervised person* will be dependent on the information that is provided by the legal person. When determining the risk assessment for a legal person (section 3.3 of *this Handbook*), the risk factors set out in section 3.3.4.1 of *this Handbook* will be relevant. The risk factors set out in section 8.2.1 of *this Handbook* will also be relevant in determining whether it is appropriate to use information on a legal person provided through, for example, a *TCSP*. In addition, the monitoring measures maintained by a *supervised person* (section 6 of *this Handbook*) may provide additional comfort that relevant and up to date information on identity has been found out.

183. Where a director of a company holds their role by virtue of their employment by (or position in) a business that is a supervised Jersey *TCSP*, separate provision is made for obtaining evidence of identity. Similar provision is made for a council member of a foundation and for a partner of a partnership.

184. Article 2 of the *Money Laundering Order*, which describes those persons considered to be *beneficial owners* of a body corporate or a *limited liability company,* provides that no individual is to be treated as a *beneficial owner* of a person that is a body corporate or a *limited liability company*, the securities of which are listed on a *regulated market*.

185. The measures that must be applied to obtain evidence of identity of beneficiaries and persons in whose favour the council of a foundation may exercise discretion, and that have been identified as presenting higher risk, will necessarily reflect the verification methods that are available at a particular time to the *supervised person*. For example, it may not be appropriate to request evidence directly from a person in whose favour discretion may be exercised.

186. Where a *supervised person* is not familiar with a document obtained to verify identity, appropriate measures may be necessary to satisfy itself that the evidence is genuine.

4.5.1 Finding out identity – Legal person that is a company

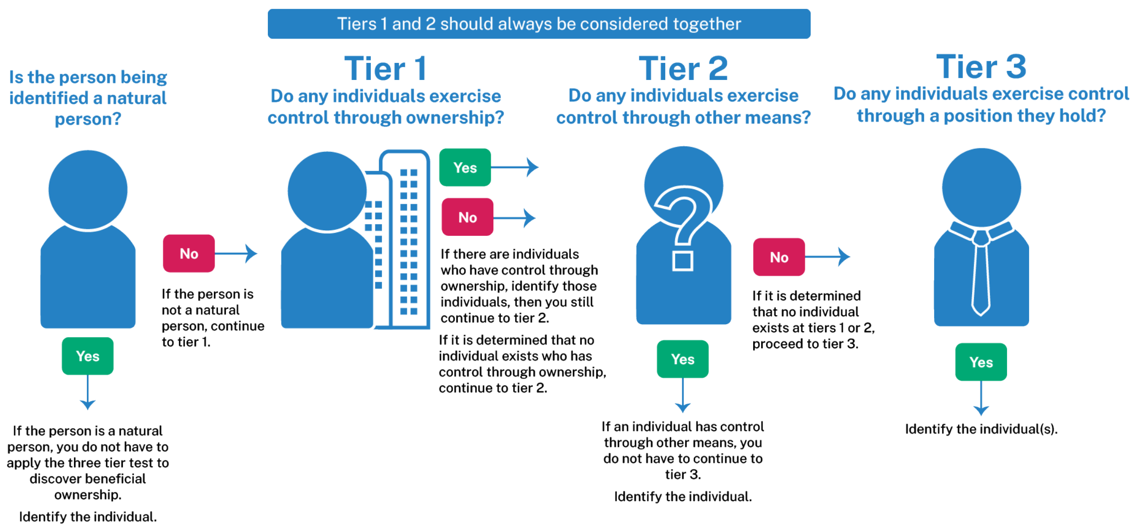
Guidance notes

187. A *supervised person* may demonstrate that it has found out the identity of a company which is a *customer* under Article 3(2)(c)(iii) of the *Money Laundering Order* where it collects all of the following:

- name of company;
- any trading names;
- date and country/territory of incorporation/registration;
- official identification number;
- registered office address;
- mailing address (if different);
- principal place of business/operations (if different); and
- names of all persons holding a senior management position.

188. To ascertain whose identity must be found out i.e., who is/are the *customer*'s *Beneficial owner and/or controllers* under Article 3(2)(c)(iii) of the *Money Laundering Order*, a *supervised person* can use a tool that is commonly known as the "Three Tier Test". The "Three Tier Test" (explanatory text and flow-chart below) relates to legal persons (e.g., companies, incorporated partnerships etc.). Individuals at Tiers 1 and 2 should be identified, and only if there are no individuals at Tiers 1 and 2 do the individuals at Tier 3 need to be identified.

Three Tier Test and description of tiers:



Tier 1: A *supervised person* may demonstrate that it has found out the identity of a person who is the *customer*'s *Beneficial owner and/or controller* under Article 3(2)(c)(iii) of the *Money Laundering Order* where it finds out the identity of persons holding a **material controlling ownership interest** in the capital of the company (through direct or indirect holdings of interests or voting rights) or who **exert control through other ownership interests**, e.g. shareholders' agreements, power to appoint *senior management*, or through holding convertible stock or any outstanding debt that is convertible into voting rights; and

Tier 2: To the extent that there is doubt as to whether the persons exercising **control through ownership** are *beneficial owners*, or where no person exerts control through ownership, a *supervised person* may demonstrate that it has found out the identity of a person who is the *customer's Beneficial owner and/or controller* under Article 3(2)(c)(iii) of the *Money Laundering Order* where it finds out the identity of those who exercise **control through other means**, e.g. those who exert control through personal connections, by participating in financing, because of close family relationships, historical or contractual associations or as a result of default on certain payments. This effectively means anyone exercising control through ownership and anyone exercising control through other means must be identified (Tier 1 and Tier 2); or

Tier 3: Where no person is otherwise identified under Tier 1 or Tier 2 above, a *supervised person* may demonstrate that it has found out the identity of a person who is the *customer's Beneficial owner and/or controller* under Article 3(2)(c)(iii) of the *Money Laundering Order* where it finds out the identity of persons who exercise **control through positions held** (e.g. those who have and exercise strategic decision-taking powers and exercise executive control through senior management positions). In the case of other bodies, anstalts, associations, clubs, societies, charities, church bodies, institutes, mutual or friendly societies, co-operatives, and provident societies, 'senior management' will often include members of the *Governing body* or committee plus executives.

189. The above information may be provided by the company.

190. In any case where a person identified is not an individual, a *supervised person* may demonstrate that it has identified each individual who is that person's *Beneficial owner and/or controller* under Article 3(2)(c)(iii) of the *Money Laundering Order* where it has identified:

i) each individual with a **material controlling ownership interest** in the capital of the company (through direct or indirect holdings of interests or voting rights) or who exerts **control of the company through other ownership means**;

i. to the extent that there is doubt as to whether the individuals exercising control through ownership are beneficial owners, or where no individual exerts control through ownership, any other individual exercising control over the company through other means. This effectively means that anyone exercising control through ownership and anyone exercising control through other means must be identified;

ii. where no individual is otherwise identified under sub-paragraphs (i) and (ii), individuals who exercise control of the company through positions held (e.g., those who have and exercise strategic decision-taking powers and exercise executive control through senior management positions).

191. In the case of a lower risk relationship, person(s) holding a senior management position who have and exercise authority to operate a *business relationship* or *one-off transaction* will be those who exercise control through positions held.

192. For lower risk relationships, a general threshold of 25% is considered to indicate a **material controlling ownership interest** in the capital of a company. Where the distribution of interests is uneven, the percentage where effective control may be exercised (a material interest) may be less than 25% when the distribution of other interests is considered.

4.5.2 Obtaining evidence of identity – Legal person that is a company

AML/CFT/CPF Codes of Practice

[COP44] All key documents (or parts thereof) obtained as evidence of identity must be understandable (i.e., in a language understood by an employee of the *supervised person*) and must be translated into English at the request of the *FIU* or the *JFSC*.

Guidance notes

193. A *supervised person* may demonstrate that it has obtained evidence under Article 3(2)(a) of the *Money Laundering Order* that is reasonably capable of verifying that a company which is a *customer* to be identified is who it is said to be where the evidence covers all the following components of identity:

- › name of company;
- › date and country/territory of incorporation/registration;
- › official identification number;
- › registered office address; and
- › principal place of business/operations (where different to registered office).

194. However, in the case of a lower risk relationship, a *supervised person* may demonstrate that it has obtained evidence under Article 3(2)(a) of the *Money Laundering Order* that is reasonably capable of verifying that a company which is a *customer* to be identified is who it is said to be where the evidence covers the following components of identity:

- › name of company;
- › date and country/territory of incorporation/registration;
- › official identification number.

195. A *supervised person* may demonstrate that it has obtained evidence under Article 3(2)(a) of the *Money Laundering Order* that is reasonably capable of verifying that a company which is a *customer* to be identified is who it is said to be where it obtains, in every case, the Memorandum and Articles of Association (or equivalent), or a copy of such documents certified by a suitable certifier, and one or more sources of further evidence (one source for lower risk *customers*):

- › certificate of incorporation (or other appropriate certificate of registration or licensing), or copy of such a certificate certified by a suitable certifier; and/or
- › latest audited financial statements or copy of such statements certified by a suitable certifier.

196. A *supervised person* may also demonstrate that it has obtained evidence under Article 3(2)(a) of the *Money Laundering Order* that is reasonably capable of verifying that a company which is a *customer* is who it is said to be where the data or information comes from an independent data source (see section 4.3.4 of *this Handbook*) or, in the case of a principal place of business, by a personal visit to that address. An independent data source may include a company registry search, which confirms that the company is not in the process of being dissolved, struck off, wound up or terminated.

197. Where a person in a senior management position holds their role by virtue of their employment by (or position in) a business that is a supervised Jersey's *TCSP*, a *supervised person* may demonstrate that it has taken reasonable measures to find out the identity of that person and to obtain evidence under Article 3(2)(c)(iii) of the *Money Laundering Order* where it obtains the following:

- the full name of the director;
- an assurance from the *TCSP* that the individual is an officer or employee.

4.5.3 Finding out identity – Legal person that is a foundation

Guidance notes

198. A *supervised person* may demonstrate that it has found out the identity of a foundation which is a *customer* under Article 3(2)(a) of the *Money Laundering Order* where it collects all the following:

- name of foundation;
- date and country/territory of incorporation;
- official identification number;
- business address. In the case of a foundation incorporated under the *Foundations Law*, this will be the business address of the qualified member of the council;
- mailing address (if different);
- principal place of business/operations (if different); and
- names of all council members and, if any decision requires the approval of any other person, the name of that person.

199. A *supervised person* may demonstrate that it has found out the identity of the foundation's *Beneficial owners and controllers* under Article 3(2)(c)(iii) of the *Money Laundering Order* where it finds out the identity of:

- the founder, a person (other than the founder of the foundation) who has endowed the foundation (directly or indirectly), and, if any rights a founder of the foundation had in respect of the foundation and its assets have been assigned to some other person, that person;
- the guardian (who takes such steps as are reasonable to ensure that the council of the foundation carries out its functions);
- the council members and, if any decision requires the approval of any other person, that person;
- any beneficiary entitled to a benefit under the foundation in accordance with the charter or the regulations of the foundation;
- any other beneficiary and person in whose favour the council may exercise discretion under the foundation in accordance with its charter or regulations and that have been identified as presenting higher risk;
- any other person exercising ultimate effective control over the foundation.

200. The above information may be provided by the foundation.

201. In any case where a founder, guardian, beneficiary, or other person listed in paragraph 192 above (the "person") is not an individual, a *supervised person* may demonstrate that it has identified each individual who is the person's *beneficial owner or controller* under Article 3(2)(c)(iii) of the *Money Laundering Order* where it has identified:

i. each individual with a **material controlling ownership interest** in the capital of the person (through direct or indirect holdings of interests or voting rights) or who exerts control through **other ownership means**;

ii. to the extent that there is doubt as to whether the individuals exercising control through ownership are beneficial owners, or where no individual exerts control through ownership, any other individual exercising **control** over the person **through other means**. This effectively means that anyone exercising control through ownership and anyone exercising control through other means must be identified;

iii. where no individual is otherwise identified under sub-paragraphs (i) and (ii), individuals who exercise control of the person **through positions held** (e.g., those who have and exercise strategic decision-taking powers and exercise executive control through senior management positions).

Refer to the flow-chart at section 4.5.1 of *this Handbook* for a graphical explanation of the process described in the paragraph above.

202. In the case of a lower risk relationship, as an alternative to finding out the identity of all council members (and, if any decision requires the approval of any other person, that person), a *supervised person* may find out the identity of council members who have and exercise authority to operate a *business relationship* or *one-off transaction*.

203. For lower risk relationships, a general threshold of 25% is considered to indicate a **material controlling ownership interest in capital**. Where the distribution of interests is uneven, the percentage where effective control may be exercised (a material interest) may be less than 25% when the distribution of other interests is considered.

4.5.4 Obtaining evidence of identity – Legal person that is a foundation

AML/CFT/CPF Codes of Practice

[COP45] All key documents (or parts thereof) obtained as evidence of identity must be understandable (i.e., in a language understood by an employee of the *supervised person*) and must be translated into English at the request of the *FIU* or the *JFSC*.

Guidance notes

204. A *supervised person* may demonstrate that it has obtained evidence under Article 3(2)(a) of the *Money Laundering Order* that is reasonably capable of verifying that a foundation which is a *customer* is who it is said to be where the evidence covers all of the following components of identity:

- name of foundation;
- date and country/territory of incorporation;
- official identification number;
- business address; and
- principal place of business/operations (if different).

205. However, in the case of a lower risk relationship, a *supervised person* may demonstrate that it has obtained evidence under Article 3(2)(a) of the *Money Laundering Order* that is reasonably capable of verifying that a foundation which is a *customer* to be identified is who it is said to be where the evidence covers the following components of identity:

› name of foundation;

› date and country/territory of incorporation;

› official identification number.

206. A *supervised person* may demonstrate that it has obtained evidence under Article 3(2)(a) of the *Money Laundering Order* that is reasonably capable of verifying that a foundation to be identified is who it is said to be where it obtains, in every case, the foundation charter (or equivalent) or a copy of such document certified by a suitable certifier, and one or more sources of further evidence (one source for lower risk *customers*):

› latest audited financial statements or a copy of such statements certified by a suitable certifier.

207. A *supervised person* may also demonstrate that it has obtained evidence under Article 3(2)(a) of the *Money Laundering Order* that is reasonably capable of verifying that a foundation which is a *customer* is who it is said to be where the data or information comes from an independent data source (see section 4.3.4 of *this Handbook*) or (in the case of a principal place of business) personal visit to that address. An independent data source may include a registry search on the *JFSC*'s website (for the business address of the qualified member of the council).

208. Where a council member who is an individual holds their role by virtue of their employment by (or position in) a business that is a *supervised Jersey TCSP*, a *supervised person* may demonstrate that it has taken reasonable measures to find out the identity of that person and to obtain evidence under Article 3(2)(c)(iii) of the *Money Laundering Order* where it obtains the following:

› the full name of the council member; and

› an assurance from the *TCSP* that the individual is an officer or employee.

4.5.5 Finding out identity – Legal Person that is a partnership

Guidance notes

209. A *supervised person* may demonstrate that it has found out the identity of a partnership which is a *customer* under Article 3(2)(a) of the *Money Laundering Order* where it collects all of the following:

› name of partnership;

› any trading names;

› date and country/territory of incorporation/registration;

› official identification number;

› registered office/business address;

› mailing address (if different);

› principal place of business/operations (if different); and

› names of all partners (except any limited partners that do not participate in management).

210. A *supervised person* may demonstrate that it has found out the identity of a person who is the *customer*'s *Beneficial owner and/or controller* under Article 3(2)(c)(iii) of the *Money Laundering Order* where it finds out the identity of limited partners holding a **material controlling ownership interest** in the capital of the partnership (through direct or indirect holdings of interests or voting rights) or any other person exercising **control through other ownership means**, e.g. partnership agreements, power to appoint senior management, or any outstanding debt that is convertible into voting rights.

211. To the extent that there is doubt as to whether the persons exercising control through ownership are *beneficial owners*, or where no person exerts control through ownership, a *supervised person* may demonstrate that it has found out the identity of a person who is the *customer*'s *Beneficial owner and/or controller* under Article 3(2)(c)(iii) of the *Money Laundering Order* where it finds out the identity of those who exercise **control through other means**, e.g., those who exert control through personal connections, by participating in financing, because of close family relationships, historical or contractual associations or as a result of default on certain payments. This effectively means that anyone exercising control through ownership and anyone exercising control through other means must be identified (the paragraph above and this paragraph).

212. Where no person is otherwise identified under the two paragraphs above, a *supervised person* may demonstrate that it has found out the identity of a person who is the *customer*'s *Beneficial owner and/or controller* under Article 3(2)(c)(iii) of the *Money Laundering Order* where it finds out the identity of persons who exercise **control through positions held** (e.g. those who have and exercise strategic decision-taking powers and exercise executive control through senior management positions, such as a general partner or limited partner that participates in management).

213. This information may be provided by the partnership.

214. In any case where a partner or other person referred to in paragraphs 203 to 205 is not an individual, a *supervised person* may demonstrate that it has identified each individual who is that person's *Beneficial owner and/or controller* under Article 3(2)(c)(iii) of the *Money Laundering Order* where it has identified:

i. each individual with a material controlling ownership interest in the capital of the partnership (through direct or indirect holdings of interests or voting rights) or who exerts control of the partnership through other ownership means;

ii. to the extent that there is doubt as to whether the individuals exercising control through ownership are beneficial owners, or where no individual exerts control through ownership, any other individual exercising control over the partnership through other means. This means that anyone exercising control through ownership and anyone exercising control through other means must be identified;

iii. where no individual is otherwise identified under sub-paragraphs (i) and (ii), individuals who exercise control of the partnership through positions held (e.g., those who have and exercise strategic decision-taking powers and exercise executive control through senior management positions).

Refer to the flow-chart at section 4.5.1 for a graphical explanation of the process described in the paragraph above.

215. In the case of a lower risk relationship, partners who have and exercise authority to operate a *business relationship* or *one-off transaction* will be those who exercise control through positions held.

216. For lower risk relationships, a general threshold of 25% is considered to indicate a **material controlling ownership interest** in the capital of a partnership. Where the distribution of interests is uneven, the percentage where effective control may be exercised (a material interest) may be less than 25% when the distribution of other interests is taken into account.

4.5.6 Obtaining evidence of identity – Legal person that is a partnership

AML/CFT/CPF Codes of Practice

[COP46] All key documents (or parts thereof) obtained as evidence of identity must be understandable (i.e., in a language understood by an employee of the *supervised person*) and must be translated into English at the request of the *FIU* or the *JFSC*.

Guidance notes

217. A *supervised person* may demonstrate that it has obtained evidence under Article 3(2)(a) of the *Money Laundering Order* that is reasonably capable of verifying that a partnership which is a *customer* to be identified is who it is said to be where the evidence covers all of the following components of identity:

- name of partnership;
- date and country/territory of incorporation/registration;
- official identification number;
- registered office/business address; and
- principal place of business/operations (if different).

218. However, in the case of a lower risk relationship, a *supervised person* may demonstrate that it has obtained evidence under Article 3(2)(a) of the *Money Laundering Order* that is reasonably capable of verifying that a partnership which is a *customer* to be identified is who it is said to be where the evidence covers the following components of identity:

- name of partnership;
- date and country/territory of incorporation/registration; and
- official identification number.

219. A *supervised person* may demonstrate that it has obtained evidence under Article 3(2)(a) of the *Money Laundering Order* that is reasonably capable of verifying that a partnership which is a *customer* to be identified is who it is said to be where it obtains, in every case, the partnership agreement or a copy of such an agreement certified by a suitable certifier, and one or more sources of further evidence (one source for lower risk *customers*):

- certificate of registration (where a partnership is registered) or copy of such a certificate certified by a suitable certifier; and/or
- latest audited financial statements or copy of such statements certified by a suitable certifier.

220. A *supervised person* may also demonstrate that it has obtained evidence that is reasonably capable of verifying that a partnership which is a *customer* is who it is said to be under Article 3(2)(a) of the *Money Laundering Order* where the data or information comes from an independent data source (see section 4.3.4 of *this Handbook*) or (in the case of a principal place of business) personal visit to that address. An independent data source may include a registry search, which confirms that the partnership is not in the process of being dissolved, struck off, wound up or terminated.

221. Where a partner holds their role by virtue of their employment by (or position in) a business that is a supervised Jersey *TCSP*, a *supervised person* may demonstrate that it has taken reasonable measures under Article 3(2)(c)(iii) of the *Money Laundering Order* to find out the identity of that person and to obtain evidence where it obtains the following:

- the full name of the partner;
- an assurance from the *TCSP* that the individual is an officer or *employee*.

4.5.7 Copy documentation provided by *CD regulated TCSP*

Guidance notes

222. Where information is provided by a *CD regulated TCSP* that is regulated by the *JFSC*, on a person who is a *Beneficial owner and/or controller* of a legal person (following an assessment of risk in line with paragraph 174 above), a *supervised person* may demonstrate that it has taken reasonable measures to obtain evidence of identity for that person under Article 13 of the *Money Laundering Order* where it obtains a copy of a document that is listed in paragraph 29 above from the supervised *TCSP*, along with the confirmations set out in the paragraph below.

223. The confirmations to be obtained are that:

- the *CD regulated TCSP* has seen the original document that it has copied to the *supervised person*, or the document that has been copied to the *supervised person* was provided to the *CD regulated TCSP* by a suitable certifier, or the evidential report copied to the *supervised person* has been obtained by the *CD regulated TCSP* as a result of utilising a *Digital ID* system which meets the requirements of *this Handbook*;
- the *CD regulated TCSP* is satisfied that the original document seen, or document provided to it by a suitable certifier, or documentary evidence permissible within a *Digital ID* system, provides evidence that the individual is who they are said to be; and
- the document provided to the *supervised person* is a true copy of a document (or evidential report) that is held by the *CD regulated TCSP*.

224. Alternatively, a *supervised person* may decide to make use of Article 16 of the *Money Laundering Order* - which allows reliance to be placed on *reliance identification measures* that have already been completed by an *obliged person* where evidence of identity may be held by the *obliged person*, and where the *obliged person* has a continuing responsibility to the *supervised person* in respect of record-keeping and access to records - see section 5 of *this Handbook*.

225. In both cases, the risk of placing reliance on another person to have carried out *identification measures* must be considered – either as part of an assessment of *customer* risk under Article 13 of the *Money Laundering Order*, or assessment of risk under Article 16 of the *Money Laundering Order.*

226. Nor should provision for copy documentation to be provided by a *CD regulated TCSP* be confused with "suitable certification", which is explained in section 4.2.4 of *this Handbook*.

227. For the avoidance of doubt, this is a very limited provision applying to *CD regulated TCSPs* and does not extend to other types of *supervised business*.

4.6 Control through other means

Statutory requirements (paraphrased wording)

228. *Under Article 2 (1)(b), 3(2)(b) (ii), 3 (2) (b) (iii) (C) and 3 (2) (c) of the Money Laundering Order, a relevant person must identify any person who ultimately controls or otherwise exercises control over the management of that person (whether the individual does so alone or with any other person or persons).*

Guidance notes

229. Control through other means are those persons who ultimately control or otherwise exercise control of the *customer* and must be ascertained as part of the *CDD* process. This control may be obvious at the beginning of the business relationship or one-off transaction. The *customer* may identify someone as having control through other means.

230. A person may have control through other means where they exert significant influence/control over decisions regarding the legal person or legal arrangement, such as:

- appointment or removal of management, except through application to the courts (directors, trustees, partners);
- directing or vetoing the profit share and/or capital returns of assets;
- directing or vetoing investment decisions;
- directing or vetoing the grant of options under a share or other share-based incentive scheme;
- directing or vetoing borrowing by the entity or lending by the entity which may be outside previously agreed thresholds;
- directing or vetoing fundamental changes to the entities business including adoption or amendment of the entities business plan;
- amendments to the constitutional documents (to include, but not limited to, the memorandum and articles, trust instrument/deed, partnership/shareholders agreement and/or side letters);
- terminating, dissolving, re-domiciling or converting the entity;
- directing or vetoing a decision, or exercise a right on behalf of the members/partners/shareholder;
- ownership or control of assets central to the *customer*'s business; and
- person enjoys the benefit of assets/property owned by the entity.

231. Control through other means is ultimate effective control which is more than minor influence.

232. Someone controlling by other means may include the following scenarios:

- shadow directors – someone who is not a member of the board but whom the board looks to or consults and whose views influence decisions made by the board.
- dominant individual/Recommendations almost always followed – someone who is not or is no longer a controller through ownership of a company or other legal person/arrangement

whose recommendations are followed or almost always followed by shareholders when deciding how to vote.

- person behind Strawman/Informal Nominee – The person holding the legal ownership of the controlling interest may do so without any reason for them to have that ownership interest. For example, they have no means to acquire the interest or have no professional reason for owning the company because they are unemployed, or is a non-financial services low paid employee of a high net worth individual. It appears that the individual is a strawman/informal nominee holding the interest to conceal the involvement of someone else who is the true controller.
- those who exert control through personal connections, by participating in financing, because of close family relationships, historical or contractual associations or as a result of default on certain payments (e.g. a lender taking control if a borrower defaults on a loan).
- where an investment manager is the instigator of the unit trust and manages the investments of the unit trust.
- a promoter may be the investment adviser/investment manager or may have a significant presence on the investment committee, which may indicate control by other means.
- a lender where loan/credit/financing arrangements extended are so material that the lender (through covenants) may exercise significant control, for example a lender with lien or charges over significant revenue generating assets of a company may be considered a controller or where there is a default on payments and the lender takes control. Lending alone without control does not amount to control by other means. For example, a bank takes out customary covenants but has no absolute veto over strategy – the bank is not a controller by other means.

These examples are not exhaustive and are intended to assist firms in applying judgement on a risk-based approach and should not be treated as a prescriptive checklist.

233. Where control through other means does not become apparent until after a relationship has been established it should be regarded as a trigger event, see section 6 – Ongoing Monitoring. In some cases when control through other means is uncovered it may have been used to try and conceal involvement of someone who is a PEP/a sanctioned individual, or someone involved in criminal activity. Good practice would be for *supervised persons* to document what steps they have taken to ascertain whether any individual exerts control by other means. The rationale for control through other means should be documented and considered and where appropriate consideration should be given to raising a *SAR*.

234. On their own, the following roles would not be considered as exercising control through other means:

- professional advisers – lawyers, accountants, management consultants, investment managers, tax advisers, financial advisers;
- third party commercial contractors – suppliers, *customer*s, lenders;
- exercise of statutory function- regulatory, liquidator, viscount or receiver;
- those acting in the course of their employment – Managing director, sole director or NED who holds a casting vote; and
- employee casting votes on behalf of group of employees.

All of the people in the roles listed above may have significant influence/control over an entity if:

- role or relationship differs in material respects or contains significantly different features from how the role or relationship is generally understood; or
- If the role or relationship forms one of several opportunities which that person has to exercise significant influence or control.

233. An example of how an entity might demonstrate and document it has taken reasonable steps to ascertain if there is control by other means.

235. Examples of good practice in identifying control by other means:

› Ask the customer to identify all controllers (including controllers by other means).

› Confirm any persons hold absolute rights to approve/veto:

- business plan/budget; nature of business; major M&A; or
- indebtedness beyond limits; appointment/removal of CEO or majority board;

If yes, record as control by other means.

› Is there a shareholders'/concert party agreement that ensures outcomes?

If yes, record as control by other means.

› Is there a de facto decision maker whose directions the board follows?

If yes, record as control by other means.

› Is control exerted via an intermediate entity (majority stake chain)?

If yes, record as control by other means.

› Is the entity controlled by a trust/foundation and does a person hold decisive powers (protector/settlor with powers etc.)?

If yes, record as control by other means.

› Apply safe harbours: professional advisers; standard commercial leverage; directors in normal role; routine lender covenants.

If only these, there may not be control by other means in isolation.

› If no one qualifies after reasonable steps and no suspicion, there may not be control by other means.

4.7 Obligation to find out identity and obtain evidence: Person purporting to act for the *customer*

Statutory requirements (paraphrased wording)

236. *Under Article 3(2)(aa) of the Money Laundering Order, a relevant person must identify any person purporting to act on behalf of the customer and verify the authority of any person purporting so to act.*

237. *Article 13 of the Money Laundering Order requires a relevant person to find out the identity of persons purportedly authorised to act on behalf of a customer that is a legal person and to take reasonable measures to obtain evidence of identity of such persons. This will include account signatories and those to whom powers of attorney have been granted in addition, Article 13 of the Money Laundering Order requires a relevant person to verify the authority of any person purporting to so act.*

238. *Article 18 of the Money Laundering Order allows this particular identification measure (or part of the identification measure) to be simplified in some limited cases.*

AML/CFT/CPF Codes of Practice

[COP47] In a case where another person purports to act on behalf of a *customer*, a *supervised person* must obtain a copy of the power of attorney or other authority or mandate that provides the persons representing the *customer* with the right to act on its behalf.

[COP48] In the case of a legal arrangement that is a trust, a *supervised person* must obtain evidence that any person purporting to act as the trustee has authority to act in such capacity.

[COP49] In the case of a legal arrangement that is a limited partnership, a *supervised person* must obtain evidence that any person purporting to act as general partner has authority to act in such capacity.

Guidance notes

239. Evidence of authority to act may include:

- obtaining a certified copy of the power of attorney;
- obtaining a certified copy of the limited partnership agreement; or
- checking records held in the companies registry regarding the identity of the general partner.

240. A *supervised person* may demonstrate that it has taken reasonable measures to obtain evidence of identity where it considers factors such as the risk posed by the relationship and the materiality of the authority delegated to individuals.

241. In the case of a lower risk relationship, a *supervised person* may demonstrate that it has taken reasonable measures to obtain evidence of identity where it does so for a minimum of two individuals that have purported authority to act on behalf of a *customer*.

4.8 Assessing complex structures

Statutory requirements (paraphrased wording)

242. *Under Article 3(2)(c)(ii) of the Money Laundering Order a relevant person is required to understand the ownership and control structure of that customer and the provisions under which the customer can enter into contracts, or other similar legally binding arrangements, with third parties. A relevant person under Article 3(2)(d) of the Money Laundering Order is required to obtain information on the purpose and intended nature of the business relationship or one-of transaction and use this information to ensure the transactions are consistent with the knowledge of the customer, including the customer's business and risk profile (Article 3(3)).*

243. *Also, under Article 11(12) of the same Order, a relevant person, when considering the type and extent of the testing to be carried out under paragraph (11), shall have regard to the risk of money laundering that exists in respect of the relevant person's business, and matters that may have an impact on that risk, such as the size and nature and structure of the relevant person's business.*

Guidance notes

244. Some customer structures may appear complex. Complexity may arise for legitimate commercial, legal, or tax planning reasons. Complexity is recognised as context-sensitive: a structure that might be perceived as complex in one sector or circumstance, may be common and considered business-as-usual in another. Where it is evident that no multi-layer ownership or control exists and parties are not linked to complex structures (e.g. natural persons opening personal products, sole traders, simple partnerships), a supervised person would not ordinarily be expected to undertake an assessment of complexity.

245. Where structural features that appear complex are common within the sector and have a clear, understood rationale, CDD may be sufficient notwithstanding other risk factors. Supervised persons are not required to treat all complex arrangements as high-risk but should assess whether the structure is transparent and consistent with its stated purpose and sector norms. Supervised persons may, where appropriate, provide staff guidance on sector-typical features with legitimate rationales. Where features are unusual for the sector, or complexity creates opacity, supervised persons should consider whether enhanced CDD measures are warranted (see Section 7).

246. Complexity alone does not automatically equate to higher ML/TF/PF risk. Some guidance on what might potentially be a complex structure is required to avoid the anomalous result of an assessment of complexity having to be made in relation to every customer which would not be efficient, or risk based.

247. The following types of indicators may point to complexity (this is a non-prescriptive, non-exhaustive list):

› multiple ownership/control layers (typically three or more ownership/control layers between the customer and the beneficial owner(s)).

› multi-jurisdictional features (place of incorporation/formation or, where relevant, tax residence) (typically three or more).

use of different types of legal persons and/or arrangements (typically three or more).

› complicated ownership/control rights (e.g. differential economic and voting rights, multiple share classes/series, carried interest waterfalls)

› fragmented administration (multiple service providers across key layers).

› transactional/payment flows that are complex for the stated business model, difficult to trace or explain, or pass through higher-risk countries without a clear commercial purpose.

248. in line with the *Handbook's* overarching risk-based approach, supervised persons must assess the actual ML/TF/PF risk having regard to:

› the transparency of ownership and control;

› the jurisdictions involved (incorporation/formation, tax residence, etc) and the availability/reliability of ownership/filing information;

› the nature of the customer's business and purpose of the relationship (including fund flows); and

› the quality and effectiveness of mitigating measures already applied.

249. A supervised person should consider as part of its customer risk assessment whether any potential complexity (within the customer or relevant linked arrangements) aligns with:

› the customer's risk profile;

› the purpose and intended nature of the relationship;

› the beneficial ownership and control information obtained; and

› the source of funds and where applicable source of wealth.

250. Where potential complexity is identified, and standard CDD measures establish the rationale for the structuring is clear and beneficial ownership adequately evidenced and verified, a supervised person should record that conclusion and may determine no further due diligence is required. If, after applying standard CDD measures, the rationale for the structuring remains unclear and/or verification of beneficial ownership and control is incomplete and requires further enquiry, the relationship may be deemed higher-risk and require enhanced CDD measures proportionate to the reason for the risk to be applied (See Section 7). This supports transparency and demonstrates that the supervised person has applied a considered and proportionate approach.

4.9 Timing of *identification measures*

Statutory requirements (paraphrased wording)

Initial

251. *Article 13(1) of the Money Laundering Order requires identification measures to be applied before the establishment of a relationship or before carrying out a one-off transaction.*

252. *However, Article 13(4) of the Money Laundering Order permits evidence of identity to be obtained after the establishment of a business relationship in three cases.*

253. *The first – set out in Article 13(6) and (7) of the Money Laundering Order – is a business relationship that relates to a life insurance policy if the identification measure relates to a beneficiary under the policy and the relevant person is satisfied that there is a little risk of money laundering or the financing of terrorism occurring. Where identification measures are not completed before the establishment of a business relationship, they must be completed before any payment is made under the policy or any right vested under the policy is exercised.*

254. *The second – set out in Article 13(8) and (9) of the Money Laundering Order – is a business relationship that relates to a trust or foundation if the identification measure relates to a person who has a beneficial interest in the trust or foundation by virtue of property or income having been vested and the relevant person is satisfied that there is a little risk of money laundering or the financing of terrorism occurring. Where identification measures are not completed before the establishment of a business relationship, they must be completed before any distribution of trust property or income is made.*

255. *The third – set out in Article 13(4) of the Money Laundering Order – is where:*

› *it is necessary not to interrupt the normal course of business;*

› *there is little risk of money laundering or the financing of terrorism occurring as a result of obtaining evidence of identity after establishing the relationship;*

- *the risk of money laundering and the financing of terrorism is effectively managed;*
- *Evidence of identity is obtained as soon as reasonably practicable.*

256. *Under Articles 11(3)(fa) and (fb) of the Money Laundering Order, policies and procedures must be in place to:*

- *assess the risk of money laundering or financing of terrorism and to manage the risks in relation to the conditions under which a customer may utilise a business relationship with the relevant person before the identification of the customer has been completed, as referred to in Article 13(4) of the Money Laundering Order;*
- *ensure that there is periodic reporting to senior management to allow it to assess that appropriate arrangements are in place to address risk and to ensure that identification measures are completed as soon as reasonably practicable.*

<u>During Business relationship</u>

257. *Article 13(1)(c)(i) of the Money Laundering Order requires a relevant person to apply identification measures where it suspects money laundering or the financing of terrorism.*

258. *In addition, where a relevant person has doubts about the veracity or adequacy of documents, data or information previously obtained under CDD measures, Article 13(1)(c)(ii) of the Money Laundering Order requires that person to apply identification measures.*

<u>Existing Customers</u>

259. *Article 13(2) of the Money Laundering Order states that, where a relevant person has a business relationship with a customer that commenced before the Money Laundering Order came into force, a relevant person must apply CDD measures that are in line with the Money Laundering Order to that relationship at appropriate times.*

260. *Article 13(3) of the Money Laundering Order states that for the purposes of Article 13(2) of the Money Laundering Order "appropriate times" means -*

for the application of identification measures:

- *times that are appropriate having regard to the degree of risk of money laundering or the financing of terrorism, taking into account the type of customer, business relationship, product or transaction concerned;*
- *any time when a relevant person suspects money laundering or the financing of terrorism (unless agreed otherwise with the FIU).*

261. *Article 13(3A) of the Money Laundering Order states that an appropriate time for finding out identity (as required by Article 3(4) of the Money Laundering Order) is a date no later than 31 December 2014, or such later date as may be agreed by the JFSC on application by relevant person on or before 31 December 2014.*

262. *Article 13(3B) of the Money Laundering Order explains that a person may be considered to have found out the identity of a customer where the information that it holds in relation to a customer is commensurate to the relevant person's assessment of risk.*

<u>All cases</u>

263. *Article 14(6) of the Money Laundering Order provides that a relevant person is not required to apply any identification measures if the relevant person:*

- *suspects money laundering in respect of any business relationship or transaction with a person;*

› *reasonably believes that the application of identification measures is likely to alert the person to the relevant person's suspicions of money laundering;*

› *has made a report under procedures maintained under Article 21 to the FIU;*

› *acting with the consent of that officer, terminates or does not establish that business relationship or does not complete or carry out that transaction.*

Overview

264. Article 13(4) of the *Money Laundering Order* allows, in certain circumstances, a *supervised person* a reasonable timeframe to undertake the necessary enquiries for obtaining evidence of identity after the initial establishment of a *business relationship*. No similar concession is available for finding out identity. Where a reasonable excuse for the continued delay in obtaining evidence of identity cannot be provided, to comply with Article 14(2) of the *Money Laundering Order*, a *supervised person* must terminate the relationship (see section 4.10 of *this Handbook*).

265. *Lawyers, Accountants*, and certain other professional advisers will also need to consider sections 20.2.2 and 21.3.3 of *this Handbook,* which provide sector-specific concessions for those who are amidst ascertaining the legal position for their *customer* or performing the task of defending or representing their *customer* in legal proceedings.

266. A *business relationship* is established as soon as a *supervised person* undertakes to act in respect of that relationship, for example by receiving and accepting signed terms of business from the *customer*, or by carrying out the instructions of the *customer*, such as investing in a financial product. Funds may be received from a *customer* during establishing a *business relationship.*

AML/CFT/CPF Codes of Practice

[COP50] In a case where Article 13(4) of the *Money Laundering Order* applies, a *supervised person* may obtain evidence of identity after the initial establishment of a *business relationship* if, in addition, the following conditions are met:

› it highlights to its *customer* its obligation to terminate the business relationship at any time on the basis that evidence of identity is not obtained; and

› *money laundering*, the *financing of terrorism*, and the financing of proliferation risk is effectively managed.

[COP51] In any event, a *supervised person* must not pay away funds to an external party, other than to invest or deposit the funds on behalf of the *customer*, until such time as evidence of identity has been obtained.

Guidance notes

267. A *supervised person* may demonstrate that it has highlighted to a *customer* the obligation to terminate a *business relationship* where terms of business, which govern its relationship with its *customer*:

› encompass the termination of *business relationships* when evidence of identity is either not obtained, or the results are unsatisfactory;

› clearly state that termination may lead to a *customer* suffering loss – e.g. where funds have been invested in a *Collective investment scheme* where a forced redemption is necessary.

268. A *supervised person* may demonstrate that *money laundering*, the *financing of terrorism*, and the *financing of proliferation* risk is effectively managed where:

› *policies and procedures* establish timeframes for obtaining evidence of identity;

- the establishment of any *business relationship* benefiting from this concession has received appropriate authorisation, and such relationships are appropriately monitored so that evidence of identity is obtained as soon as is reasonably practicable; and
- appropriate limits or prohibitions are placed on the number, type and amount of transactions over an account for such relationships.

269. A *supervised person* may demonstrate that periodic reporting is in line with Article 11(3)(fa) of the *Money Laundering Order* where it highlights to the board:

- the number of *customers* for which evidence of identity has not been obtained during a reporting period (also expressed as a percentage of the total number of *business relationships* established during the reporting period) and summarises reasons;
- in any case where the delay is for more than a particular period of time, the name of the *customer*, the reason for the delay, the extent to which evidence of identity has not been obtained, the risk rating given to that *customer*, and action that is to be taken to obtain evidence or terminate the *business relationship* (and by when).

270. Guidance as to appropriate steps to take where a *supervised person* is unable to complete *identification measures* is provided in section 4.10 of *this Handbook*.

4.9.1 Timing of *identification measures* during business relationship – Obtaining evidence

Guidance notes

271. During a *business relationship* between a *supervised person* and a *customer* that is a trustee, a *supervised person* may demonstrate that it has obtained evidence that is reasonably capable of verifying the identity of each beneficiary with a vested right where:

- it does so at the time of, or before, distribution of trust property or income; and
- it is satisfied that there is little risk of *money laundering,* the *financing of terrorism,* or the *financing of proliferation* occurring because of obtaining evidence after entitlement is conferred.

272. In the course of a *business relationship* between a *supervised person* and a *customer* that is a trustee, a *supervised person* may demonstrate that it has obtained evidence that is reasonably capable of verifying the identity of a beneficiary or person who is the object of a trust power where it does so at the time that the person is identified as presenting a higher risk.

273. In the case of a *business relationship* between a *supervised person* and a *customer* that is a **foundation**, a *supervised person* may demonstrate that it has obtained evidence that is reasonably capable of verifying the identity of each beneficiary entitled to benefit under the foundation where:

- it does so at the time of, or before, distribution of property or income;
- it is satisfied that there is little risk of *money laundering*, the *financing of terrorism*, or the *financing of proliferation* occurring because of obtaining evidence after conferring entitlement.

274. In the course of a *business relationship* between a *supervised person* and a *customer* that is a **foundation**, a *supervised person* may demonstrate that it has obtained evidence that is reasonably capable of verifying the identity of any beneficiary or person in whose favour the council may exercise discretion under the foundation where it does so at the time that the person is identified as presenting a higher risk.

4.9.2 Timing for "existing *customers*"

Overview

275. *FATF Recommendation 10* states that *Financial Institutions* should be required to apply that *Recommendation* (which deals with *CDD* measures) to "existing *customers*" on the basis of materiality and risk, and should conduct *CDD* measures on such existing relationships at appropriate times. This is based on the presumption that *identification measures* applied historically to existing *customer*s will have been less effective than those to be applied in line with *FATF Recommendation 10.*

276. For the purposes of the *Money Laundering Order,* the meaning of existing *customer* depends on the sector. In the case of a *supervised business*, this means a *business relationship* established before the *Money Laundering Order* came into force on 4 February 2008 and which continues. In the case of *real estate agents, high value dealers, Accountants* and *Lawyers* this means a *business relationship* established before the *Money Laundering Order* came into force on 1 May 2008 and which continues.

277. Historically Article 13(2) of the *Money Laundering Order* allowed for deferral of *CDD* measures, specifically finding out the identity of an existing *customer* (also known as legacy *customer*s) with a relationship established before the *supervised person* was subject to *AML/CFT/CPF* requirements, subject to certain conditions. This concession became time barred on 31 December 2014 unless consent was sought from the JFSC. No such consents remain outstanding, and therefore, all existing *customer*s should have been remediated. Article 13(1)(c)(ii) of the *Money Laundering Order* will apply to such a relationship in the same way as a relationship established on or after the dates referred to in Article above, on the basis that documents, data or information on all existing/legacy *customer*s should align with the *CDD* measures prescribed in Article 3.

278. All existing/legacy *customer*s are subject to ongoing monitoring and review of *CDD* information and evidence. The requirement to review *CDD* is not limited to high-risk *customer*s.

279. Higher risk existing/legacy *customer*s will be subject to the same programme of enhanced monitoring as any new high-risk *customer*.

280. In line with Article 13(3)(a)(ii) of the *Money Laundering Order*, *identification measures* must always be applied to an existing *customer* as soon as a *supervised person* suspects *money laundering*, the *financing of terrorism*, or the *financing of proliferation.*

281. A *supervised person* may meet its obligation to apply *identification measures* by placing reliance on an *obliged person*. See section 5 of *this Handbook.*

AML/CFT/CPF Codes of Practice

[COP52] A *supervised person* must review its "existing *customer*" base to determine a risk assessment for each *customer* that has still to be remediated.

Guidance notes

282. Where it does not suspect *money laundering*, the *financing of terrorism*, the *financing of proliferation*, a *supervised person* may demonstrate that it has **found out the identity** at an appropriate time for a **higher risk** existing *customer* where it does so at the earlier of the following dates:

- as soon as is practicable after the date that a *supervised person* has assessed a *customer* to present a higher *money laundering*, the *financing of terrorism*, or the *financing of proliferation* risk; or

- 31 December 2014 (or later date agreed with the *JFSC* on application by the *supervised person* on or before 31 December 2014).

283. Where it does not suspect *money laundering*, the *financing of terrorism*, or *proliferation financing*, a *supervised person* may demonstrate that it has **found out the identity** at an appropriate time for a **standard** or **lower risk** existing *customer* where it does so at the earlier of the following dates:

- the date when a transaction of significance takes place;
- the date when a *supervised person*'s *customer* documentation standards change substantially; or
- 31 December 2014 (or later date agreed with the *JFSC* on application by the *supervised person* on or before 31 December 2014).

284. Where it does not suspect *money laundering*, the *financing of terrorism*, or *proliferation financing*, a *supervised person* may demonstrate that it has obtained **evidence of identity** at an appropriate time for an existing *customer* where it does so as soon as is practicable after the *customer* has been assessed as presenting a **higher risk** of *money laundering*, the *financing of terrorism*, or the *financing of proliferation*.

285. A *supervised person* may demonstrate that it has applied *identification measures* where it does so in accordance with measures applied to **new** *business relationships* and *one-off transactions*, considering any factors that are relevant to an existing relationship. Such factors could include existing knowledge of the *customer* built up through the historical conduct of the relationship, etc.

4.10 Failure to complete *identification measures*

Statutory requirements (paraphrased wording)

286. *If a relevant person is unable to apply identification measures before the establishment of a business relationship or before carrying out a one-off transaction (except in the circumstances set out in Article 13(4) of the Money Laundering Order), Article 14(1) of the Money Laundering Order requires that a relevant person shall not establish that business relationship or carry out that one-off transaction.*

287. *Article 14(2) of the Money Laundering Order requires a relevant person that is unable to apply identification measures in the circumstances described in Article 13(4) of the Money Laundering Order, to terminate the relationship.*

288. *Article 14(5) of the Money Laundering Order requires a relevant person to terminate a business relationship where it cannot apply ongoing identification measures.*

289. *Article 14(7) of the Money Laundering Order states that, if a relevant person is unable to apply identification measures to an existing customer at the appropriate time, it must terminate that particular business relationship.*

290. *Article 14(11) of the Money Laundering Order provides that a business relationship or one-off transaction may proceed or continue where a relevant person is acting with the consent of the FIU.*

Guidance notes

291. Where *identification measures* cannot be completed, a *supervised person* must not establish a *business relationship* or carry out a *one-off transaction*. In the case of an established *customer* relationship, that relationship must be terminated.

292. The timing of the termination of an established relationship will depend on the underlying nature of the *business relationship*. For example, whereas a bank can close an account relatively easily and return deposited funds to a *customer*, it may be problematic to effect a compulsory redemption of a holding of units in a *Collective investment scheme*, particularly where it is closed ended, or where valuation dates are infrequent.

293. Wherever possible, when terminating a *business relationship* where *customer* money or other assets have been received, a *supervised person* should return said assets directly to the *customer*, i.e., by returning money to the account from which it was received.

294. In a case where the *customer* requests that assets or funds be transferred to an external party, or to a different account in the *customer's* name, a *supervised person* should assess whether this provides grounds for knowledge or suspicion, or reasonable grounds for knowledge or suspicion, of *money laundering*, the *financing of terrorism, or proliferation financing*.

295. Where contact has been lost with a *customer* so that it is not possible to complete termination of a *business relationship*, assets or funds held should be "blocked" or placed on a "suspense" account until such time as contact is re-established.

5 *IDENTIFICATION MEASURES* – RELIANCE ON *OBLIGED PERSONS*

5.1 Overview of section

1. In some strictly limited cases, a *supervised person* may meet its obligation to comply with Articles 13(1)(a) or (c)(ii) (*CDD*); 15(1)(a), (b), (d), (e) or (g) (*Enhanced CDD measures*); or 15A (*Enhanced CDD Measures* in relation to *PEPs*) of the *Money Laundering Order*, and *AML/CFT/CPF Codes of Practice* by placing reliance on measures that have already been applied by an *obliged person* to find out the identity of a mutual *customer* and to obtain evidence of identity.

2. To consider what reliance might be placed on an *obliged person*, a *supervised person* will first need to determine what elements of identity must be found out and what evidence of identity is to be obtained for its *customer*. It will do so in accordance with Article 3 of the *Money Laundering Order* and the *AML/CFT/CPF Codes of Practice* set out in sections 3, 4, 6 and 7 of *this Handbook*, and will also consider its risk assessment for the *customer*. Once it has determined what *identification measures* it is to apply, a *supervised person* can then consider whether those measures have already been applied by an *obliged person*.

3. Where an *obliged person* has met its *customer*, who is resident in the same country or territory as the *obliged person*, the measures that it has taken to find out identity and to obtain evidence of identity will be different to the *identification measures* that must be applied by the *supervised person* in a case where the *supervised person* is resident in a different country or territory to the *obliged person* and *customer*, and where it has not met its *customer*. Even in a case where the *supervised person* and *obliged person* have met a *customer* and are resident in the same country or territory, the measures taken by the *obliged person* may still differ to those to be applied by the *supervised person* to the extent that other factors are different, for example, the nature of the product or service to be provided.

4. The effect of this is that the *obliged person* may not have found out all the same information on identity as the *supervised person* needs and may have obtained evidence of identity using different documents, data, or information. This means that, in practice, the scope to place reliance may sometimes be quite limited, and that it may be necessary for a *supervised person* to find out more information on identity and obtain evidence for that aspect of identity itself.

5. However, it is not necessary for the *obliged person* to have found out identity or obtained evidence of identity exactly in line with *policies and procedures* applied by the *supervised person*, since *Guidance notes* in section 4 of *this Handbook* provide that there are different ways in which to apply *identification measures*. Also, where the *obliged person* is outside Jersey, different requirements and guidance will be applicable.

6. Where an *obliged person* meets the requirements outlined in Article 16 of the *Money Laundering Order*, a *supervised person* is permitted to place reliance on the *obliged person* to have found out the identity and to have obtained evidence of the identity of:

- the *supervised person's customer*;
- any *Beneficial owner and/or controller* of that *customer*;
- any third party for which that *customer* is acting;
- any *Beneficial owner and/or controller* of a third party for whom that *customer* is acting;
- any person purporting to act on behalf of that *customer*.

7. It is not possible to place reliance on an *obliged person* to obtain information on the purpose and intended nature of a *business relationship* or *one-off transaction*, nor to apply ongoing monitoring during a *business relationship*.

8. As noted above, overall *CDD* is always required to be undertaken by the *supervised person*. However, set out below are two tables summarising the elements of *CDD* that, in the absence of other provisions, the *supervised person* is required to undertake itself:

***CDD* element**	**Always required to be undertaken by the *supervised person***
Identification measures	Risk assessment.
	Obtain information on purpose/nature.
Ongoing monitoring	Scrutinising transactions/activity.
	Keep documents/information up to date.

<table>
<tr><th>CDD element</th><th colspan="2">Article 16(2) of the Money Laundering Order allows reliance upon an obliged person</th></tr>
<tr><td rowspan="5">Identification measures</td><td colspan="2">Identify customer.</td></tr>
<tr><td colspan="2">Identify third parties.</td></tr>
<tr><td>Identify person acting for customer.</td><td>Verify authority to act.</td></tr>
<tr><td rowspan="2">Where customer not individual:</td><td>Understand ownership/control structure.</td></tr>
<tr><td>Identify Beneficial owners/controllers.</td></tr>
</table>

9. Article 16 of the *Money Laundering Order* cannot be applied in any case where:

- a supervised person suspects money laundering, the financing of terrorism, or proliferation financing;
- a *supervised person* considers that there is a higher risk of *money laundering,* the *financing of terrorism*, or *proliferation financing* based on a risk assessment carried out under Article 16(4) of the *Money Laundering Order* (see section 5.1.1 of *this Handbook*); or
- the obliged person has a relevant connection to an enhanced risk state (see section 7.5 of this Handbook).

10. Whilst the information on **identity found out** by the *obliged person* must be provided to the *supervised person* immediately before establishing a *business relationship* or carrying out a *one-off transaction*, a *supervised person* is not also required to immediately obtain **evidence of identity**. Evidence of identity may be held by an *obliged person*, so long as the *supervised person* is satisfied that the *obliged person* will provide the evidence that it holds, on request and without delay. However, it is not uncommon for evidence of identity to be called for at the same time as information on identity is provided by the *obliged person*.

11. **Examples of *obliged persons*** include, but are not limited to:

- an investment advisor who arranges for a *customer* to invest in a financial product provided by a *supervised person*, where the investment is to be held in the name of the *customer* and not that of the investment advisor;
- a *Trust Company Business* that establishes a bank or investment account for a client company, trust or foundation;
- a law firm that is a *supervised person* carrying on *supervised business;*

- an accountancy firm that is a *supervised person* carrying on *supervised business*.

12. A *supervised person* will remain responsible for the satisfactory performance of all elements of *reliance identification measures*.

13. However, where the measures taken by a *supervised person* are reasonable, it will have a defence should the *obliged person* fail to have performed satisfactory measures.

14. Outsourcing arrangements and the appointment of *AMLSP* to provide *AMLSP* services (*AMLSP* arrangements) are not included within the scope of this section, as these are distinct from circumstances in which reliance is placed on an *obliged person*. In an outsourcing arrangement/*AMLSP* arrangement, notwithstanding that the service provider may have substantial contact with the *customer*, the *customer*'s direct relationship is with the *supervised person.* The service provider will perform the outsourced/*AMLSP services* on behalf of the *supervised person* according to the terms of a contract with the *supervised person*. An example of a typical outsourcing arrangement is where a trustee of a *Collective investment scheme* outsources the management of the scheme to an external party.

15. Whether a *supervised person* in receipt of outsourced services/*AMLSP services* can be an *obliged person* will need to be assessed on a case-by-case basis, noting that while a *supervised person* using an *AMLSP* may be an *equivalent business*, it will not be a *regulated business*.

16. Where information on identity is found out, or evidence of that identity, is passed by an *obliged person* to a *supervised person* to comply with requirements to counter *money laundering* and the *financing of terrorism,* the Data Protection (Jersey) Law 2018 restricts the use of the information to that purpose, except where another condition for processing personal data applies.

17. A *customer* may be an individual (or group of individuals) or a legal person. Section 4.3 of *this Handbook* deals with a *customer* who is an individual (or group of individuals), section 4.4 of *this Handbook* deals with a *customer* (an individual or legal person) who is acting for a legal arrangement, and section 4.5 of *this Handbook* deals with a *customer* who is a legal person.

18. Under Article 16(1) of the *Money Laundering Order*, in this section "*customer of the obliged person*" means:

- a *customer* of the *obliged person*;
- a *Beneficial owner and/or controller* of that *customer*;
- a third party for whom that *customer* is acting;
- a *Beneficial owner and/or controller* of a third party for whom that *customer* is acting;
- a person purporting to act on behalf of that *customer*.

Statutory requirements (paraphrased wording)

19. *In some strictly limited circumstances, Article 16(2) of the Money Laundering Order provides that a relevant person may be considered to have applied the reliance identification measures where such measures have already been applied by an obliged person. Obliged person means a person who the relevant person knows or has reasonable grounds for believing is:*

- *a relevant person in respect of whom the JFSC discharges supervisory functions that is overseen for AML/CFT compliance in Jersey;*
- *a person who carries on equivalent business (refer to section 1.9 of this Handbook).*

20. *Reliance must always be subject to a number of conditions.*

21. *The first condition (Article 16(2)(a) of the Money Laundering Order) is that the obliged person consents to being relied upon.*

22. *The second condition (Article 16(4) of the Money Laundering Order) is that identification measures have been applied by the obliged person in the course of an established business relationship or one-off transaction.*

23. *The third condition (Article 16(4)(a),(b),(c) and (d) of the Money Laundering Order) is that the relevant person obtains adequate assurance in writing that the obliged person:*

- *has applied reliance identification measures in relation to the customer;*
- *has not itself relied upon another party to have applied any reliance identification measures;*
- *has not, in reliance on any provision in Part 3A of the Money Laundering Order (or if the obliged person is not in Jersey, a provision of similar effect), applied measures that are less than equivalent to the reliance identification measures;*
- *is required to keep, and does keep, evidence of the identification as described in Article 3(4)(b) of the Money Laundering Order relating to each of the obliged person's customers, including a record of such evidence.*

24. *The fourth condition (Article 16(2)(b) of the Money Laundering Order) is that the obliged person immediately provides the relevant person with the information obtained from applying the reliance identification measures.*

25. *To the extent that reliance is placed on an obliged person to keep hold of the evidence obtained under reliance identification measures, the fifth condition (Article 16(5) of the Money Laundering Order) is that the relevant person obtains adequate assurance in writing that the obliged person will:*

- *keep that evidence until the evidence has been provided to the relevant person, or until notification is received from the relevant person that the evidence is no longer required to be kept;*
- *provide that evidence to the relevant person at its request, and without delay.*

26. *The sixth condition (Article 16(3) of the Money Laundering Order) is that, immediately before placing reliance, the relevant person assesses the risk of placing reliance and makes a written record as to the reason why it is appropriate for it to place reliance on the obliged person, having regard to:*

- *the higher risk of money laundering or the financing of terrorism should the obliged person fail to carry out any action specified in the assurances obtained under paragraphs 23 and 25 above;*
- *the risk that an obliged person will fail to provide the relevant person with evidence without delay if requested to do so by the relevant person. See section 5.1.1 of this Handbook.*

27. *Under Article 16(8) of the Money Laundering Order a relevant person who relies on an obliged person under this Article must conduct tests in such manner and at such intervals as the relevant person considers appropriate in all the circumstances to establish whether:*

- *the obliged person has appropriate and consistent policies and procedures in place to apply reliance identification measures;*
- *if the obliged person has not already provided the evidence to the relevant person, the obliged person does keep the evidence they have obtained during the course of applying reliance identification measures in respect of a person;*

› *the obliged person will provide that evidence without delay if requested to do so.*

28. *Under Article 16(8)(c) of the Money Laundering Order, testing should take into consideration whether the obliged person may be prevented, by application of law, from providing information or evidence, e.g. secrecy legislation.*

29. *If, as a result of carrying out any such test, a relevant person is not satisfied that the obliged person has appropriate and consistent policies and procedures in place, keeps evidence, or will provide it without delay if requested to do so, in that particular case, Article 16(9) of the Money Laundering Order requires the relevant person to apply reliance identification measures immediately.*

30. *Article 16(6)(a) of the Money Laundering Order provides that a written assurance will be adequate if it is reasonably capable of being regarded as reliable and a relevant person is satisfied that it is reliable.*

31. *Article 16(6)(b) of the Money Laundering Order provides that written assurances may be provided each time that reliance is placed or through a more general arrangement with an obliged person that has an element of duration, e.g. terms of business.*

32. *Article 16(7) of the Money Laundering Order states that a relevant person (including a person who was formerly a relevant person) who has given an assurance to another person under Article 16 (5) of the Money Laundering Order (or under an equivalent provision that applies outside Jersey) must, if requested by the other person, provide the person with the evidence obtained from applying the reliance identification measures.*

33. *Article 16(11) of the Money Laundering Order states that nothing in this Article permits a relevant person to rely on the reliance identification measures of an obliged person if:*

› *the relevant person suspects money laundering or the financing of terrorism;*

› *the relevant person considers that there is a higher risk of money laundering on the basis of the assessment made under Article 16(3) of the Money Laundering Order;*

› *the obliged person is a person having a relevant connection with an enhanced risk state (within the meaning of Article 15 of the Money Laundering Order).*

34. *Notwithstanding that reliance may be placed on an obliged person, Article 16(10) of the Money Laundering Order states that a relevant person is liable for any failure to apply reliance identification measures.*

AML/CFT/CPF Codes of Practice

[COP53] To the extent that reliance is placed on an *obliged person*, a *supervised person* must be able to demonstrate that the conditions required by the *Money Laundering Order* are met.

[COP54] All evidence of identity passed by the *obliged person* to a *supervised person* (on request) must be confirmed by the *obliged person* as being a true copy of either an original or copy document held on its file.

Guidance notes

Assurance in writing about *reliance identification measures*

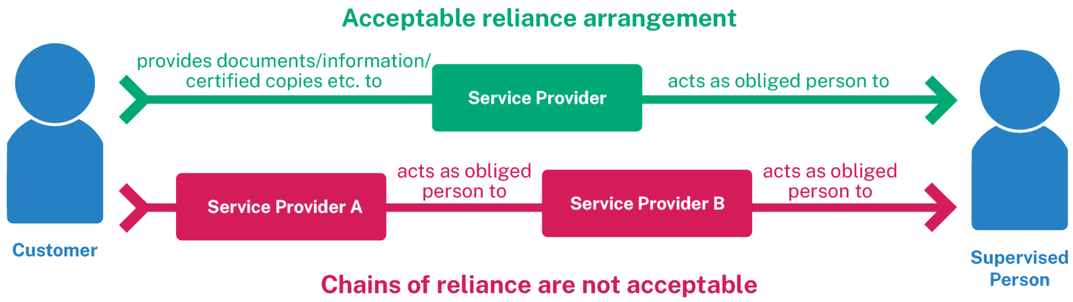
35. A *supervised person* may demonstrate that it has obtained adequate assurance in writing from an *obliged person* under Article 16(4)(a) of the *Money Laundering Order* that it has applied *reliance identification measures* to the *customer*, where the *obliged person*:

› provides information on **identity** that it has **found out** using an information template; and

› explains what **evidence of identity** it has obtained.

36. An assurance that addresses the matters listed in paragraph 35 above will be reasonably capable of being regarded as reliable under Article 16(6)(a) of the *Money Laundering Order*.

37. As stated at Article 16(4)(b) of the *Money Laundering Order* and referenced in the *statutory requirements* section above, a *supervised person* must not rely on an *obliged person* who is in turn relying on someone else (also known as a chain of reliance). See the diagram below for a graphical explanation of this point.



38. Where, as a result of Article 16(6)(b) of the *Money Laundering Order*, a *supervised person* has a more general arrangement with an *obliged person*, such as terms of business, that more general arrangement may be used to explain what **evidence of identity** will routinely be obtained by the *obliged person.*

Access to evidence of identity

39. A *supervised person* will have demonstrated that an *obliged person* is providing evidence of identity without delay if it is provided within **two working days**. If it is provided later than **five working days**, it is not provided without delay. If it is provided **between two and five working days**, the *supervised person* must be able to show why this constitutes provision without delay based on the nature of its *customer* base. In order to demonstrate that it has adequately assessed a delay, the *supervised person* is expected to provide detail of the reasons for the delay, how many days evidence remained outstanding, how many times a delay has occurred previously across the *supervised person's* practice, as well as the board/senior management's considerations.

5.1.1 Assessment of risk

Overview

40. The risk factors that are set out in this section will also be relevant to a *CRA* that is conducted under section 3.3.4.1 of *this Handbook*, in the cases highlighted at sections 4.3 to 4.5 of *this Handbook*.

Statutory requirements (paraphrased wording)

41. *Before relying upon the obliged person, the relevant person must assess the risk of doing so and make a written record of the reasons the relevant person considers that it is appropriate to do so, having regard to two risks.*

42. *The first is the higher risk of money laundering or the financing of terrorism should an obliged person fail to carry out any actions specified in the assurances obtained under Articles 16(4) and (5) of the Money Laundering Order.*

43. *The second is the risk that an obliged person will fail to provide the relevant person with evidence without delay if requested to do so by the relevant person.*

44. *Article 16(3) of the Money Laundering Order requires a relevant person to prepare a written record of the reason why it is appropriate to place reliance on an obliged person.*

AML/CFT/CPF Codes of Practice

[COP55] In a case where, for a particular *business relationship*, testing under Articles 16(8) and (9) of the *Money Laundering Order* highlights that an *obliged person*:

- has not applied the necessary reliance *identification measures*;
- does not provide adequate, accurate and current information;
- does not keep evidence of identity for as long as is necessary; or
- will not provide that evidence without delay when requested to do so;

a *supervised person* must review the basis upon which it has placed reliance on that *obliged person* for other relationships (if any) to determine whether it is still appropriate to do so.

Guidance notes

45. Immediately before relying upon an *obliged person*, a *supervised person* may demonstrate that it has had regard for the higher risk of *money laundering,* the *financing of terrorism,* or the *financing of proliferation*, and risk that an *obliged person* will fail to provide the *supervised person* with evidence of identity without delay if requested to do so, where it considers the following factors:

- the stature and regulatory track record of the *obliged person*;
- the risks posed by the country/territory/area in which the *obliged person* is based. Factors to consider include those found at section 3.3.4.1 of *this Handbook*;
- the adequacy of the framework to combat *money laundering,* the *financing of terrorism,* or the *financing of proliferation* in place in the country/territory/area in which the *obliged person* is based, and the period of time that the framework has been in place;
- the adequacy of the supervisory regime to combat *money laundering,* the *financing of terrorism,* or the *financing of proliferation* to which the *obliged person* is subject;
- the adequacy of *identification measures* applied by the *obliged person* to combat *money laundering*, the *financing of terrorism,* and the *financing of proliferation*.

46. A *supervised person* may demonstrate that it has considered the adequacy of *identification measures* applied by an *obliged person* where it takes one or more of the following steps:

- reviews previous experience (if any) with the *obliged person*, in particular the adequacy and accuracy of information on identity found out by the *obliged person* and whether that information is current;
- makes specific enquiries, e.g., through the use of a questionnaire or a series of questions;
- reviews relevant *policies and procedures* to combat *money laundering,* the *financing of terrorism,* and the *financing of proliferation* in place at the *obliged person*;
- where the *obliged person* is a member of a *financial group*, makes enquiries concerning the extent to which group standards are applied to and assessed by the group's internal audit function.

5.2 Group reliance

Overview

47. In some strictly limited cases, a *supervised person* may meet its obligation to comply with Articles 13(1)(a) or (c)(ii) (*CDD*); 15(1)(a), (b), (d), (e) or (g) (*Enhanced CDD Measures*); or 15A (*Enhanced CDD Measures* in relation to *PEPs*) of the *Money Laundering Order,* and the *AML/CFT/CPF Codes of Practice* by placing reliance on *similar identification measures* that have already been applied by a party outside Jersey who is a member of the same *financial group* as the *supervised person,* but is not also an *obliged person*.

48. The effect of Article 16A of the *Money Laundering Order* is therefore to extend the application of Article 16 of the *Money Laundering Order* to an 'external person' who could not otherwise be relied on, and the six conditions and provisions for testing outlined in section 5.1 of *this Handbook* apply to an external person in the same way as to an *obliged person*.

49. Under the definitions provided in Article 16A(1) of the *Money Laundering Order*, in this section 'external person' means a person outside Jersey, who:

› is not an *obliged person*;

› is a member of the same *financial group* as the *supervised person*; and

› carries on a business which, if that business were carried on in Jersey, would be a *supervised business*.

Statutory requirements (paraphrased wording)

50. *In some strictly limited circumstances, Article 16A of the Money Laundering Order provides that a relevant person may be considered to have applied similar identification measures specified in Article 3(2)(a), (aa), (b) and (c) of the Money Laundering Order where such measures have already been applied by an external person.*

51. *Under Article 16A(2)(c-f) of the Money Laundering Order, in order to place reliance on an external person, the financial group to which the relevant person and external person belong must:*

› *apply CDD measures and record-keeping requirements in line with the Money Laundering Order or in line with FATF Recommendations 10, 11 and 12;*

› *maintain a programme against money laundering and the financing of terrorism which includes policies and procedures by which every member of the group who carries on a financial services business (or equivalent) shares information that is appropriate for the purpose of preventing and detecting money laundering and the financing of terrorism (an AML/CFT programme);*

› *adequately mitigate any higher risk of money laundering and the financing of terrorism through its policies and procedures;*

› *be supervised by an overseas regulatory authority in its implementation of CDD measures and record-keeping requirements, and its AML/CFT programme.*

52. *Article 16(A)(2), (3), (4), (5) and (6) of the Money Laundering Order states that reliance is always subject to several conditions. These are outlined at paragraphs 21 to 26 above, where references to "obliged person" should be read as referring to "external person".*

53. *Articles 16(A)(7) and (8) of the Money Laundering Order state that reliance must always be subject to testing. Provisions in this respect are outlined at paragraphs 27 to 29 above, where references to "obliged person" should be read as referring to "external person".*

54. *Article 1(5) of the Money Laundering Order explains that a person is a member of the same financial group as another person if there is, in relation to the group, a parent company or other legal person that exercises control over every member of that group for the purposes of applying group supervision under:*

- *the Core Principles for Effective Banking Supervision published by the Basel Committee;*
- *the Objectives and Principles for Securities Regulation issued by IOSCO; or*
- *the Insurance Supervisory Principles issued by the IAIS.*

AML/CFT/CPF Codes of Practice

[COP56] A *supervised person* may not rely on an ‘external person’ where it suspects *money laundering*, the *financing of terrorism*, or the *financing of proliferation*, considers that there is a higher risk of *money laundering*, the *financing of terrorism* or the *financing of proliferation* on the basis of a risk assessment carried out under Article 16(3) of the *Money Laundering Order*, or where the external person has a relevant connection to an *enhanced risk state*.

[COP57] Despite a *supervised person*’s reliance on an ‘external person’ under Article 16A(9) of the *Money Laundering Order*, a *supervised person* is liable for any failure to apply *similar identification measures*.

6 ONGOING MONITORING

6.1 Obligation to perform ongoing monitoring

Statutory requirements (paraphrased wording)

1. Article 3(3) of the *Money Laundering Order* sets out what ongoing monitoring is to involve:

   › *scrutinising transactions undertaken throughout the course of a business relationship to ensure that the transactions being conducted are consistent with the relevant person's knowledge of the customer, including the customer's business and risk profile. See Article 3(3)(a) of the Money Laundering Order;*

   › *keeping documents, data, or information up-to-date and relevant by undertaking reviews of existing records, particularly in relation to higher risk categories of customers. See Article 3(3)(b) of the Money Laundering Order.*

2. *Article 13 of the Money Laundering Order requires a relevant person to apply ongoing monitoring throughout the course of a business relationship.*

6.2 Overview of ongoing monitoring

3. This section outlines the statutory provisions concerning ongoing monitoring. Ongoing monitoring consists of:

   › scrutinising transactions undertaken throughout the course of a *business relationship* and

   › keeping documents, data, or information up-to-date and relevant.

4. The obligation to monitor a *business relationship* starts at the time the business relationship is established and finishes at the time that it is terminated.

5. As part of the take on and risk assessment of any *customer*, a *supervised person* may demonstrate that it has considered the risk of the business where it considers the factors set out at Section 3.3.4.1 of *this Handbook*. In assessing these factors, reference may be made to external data sources as per Section 3.3.4.2.

6. In a case where a relationship has been terminated, but where payment for a service remains outstanding, a *supervised person* will still need to consider reporting provisions summarised in section 8 of *this Handbook*. For example, where there is suspicion that payment for the service is made from the proceeds of criminal conduct or instrumentalities. Noting that record keeping requirements extend beyond the termination of business relationships see section 11. Termination provides an opportunity to ensure *CDD* records are up to date.

7. This section explains the requirement to regularly keep *customer* documents, data, or information up-to-date and relevant to current standards and the measures required to demonstrate compliance with the requirement to scrutinise transactions and sets a requirement to scrutinise *customer* activity. Customer information and data is dynamic and need to be reassessed continuously.

8. Ongoing monitoring activities can be divided into two types:

   › Scheduled periodic reviews; and

- Monitoring activities undertaken on an ongoing basis, which includes transaction/activity monitoring, ongoing screening or business as usual notifications which may lead to a Trigger Event.

9. Screening, transaction/activity monitoring and periodic review arrangements should be properly documented *and* assessed as to whether they provide an acceptable level of risk mitigation as part of ongoing monitoring of effectiveness of compliance.

10. For some *customer*s, additional information may only become evident **during** the course of the *business relationship* (i.e., whilst acting for the *customer*), leading to a revised profile and risk assessment. This requires particular diligence and care when updating documents, data or information and when scrutinising and monitoring *customer* activity and transactions. In these cases, appropriate staff training in the recognition of unusual transactions and activity is vital, as are relevant systems and controls.

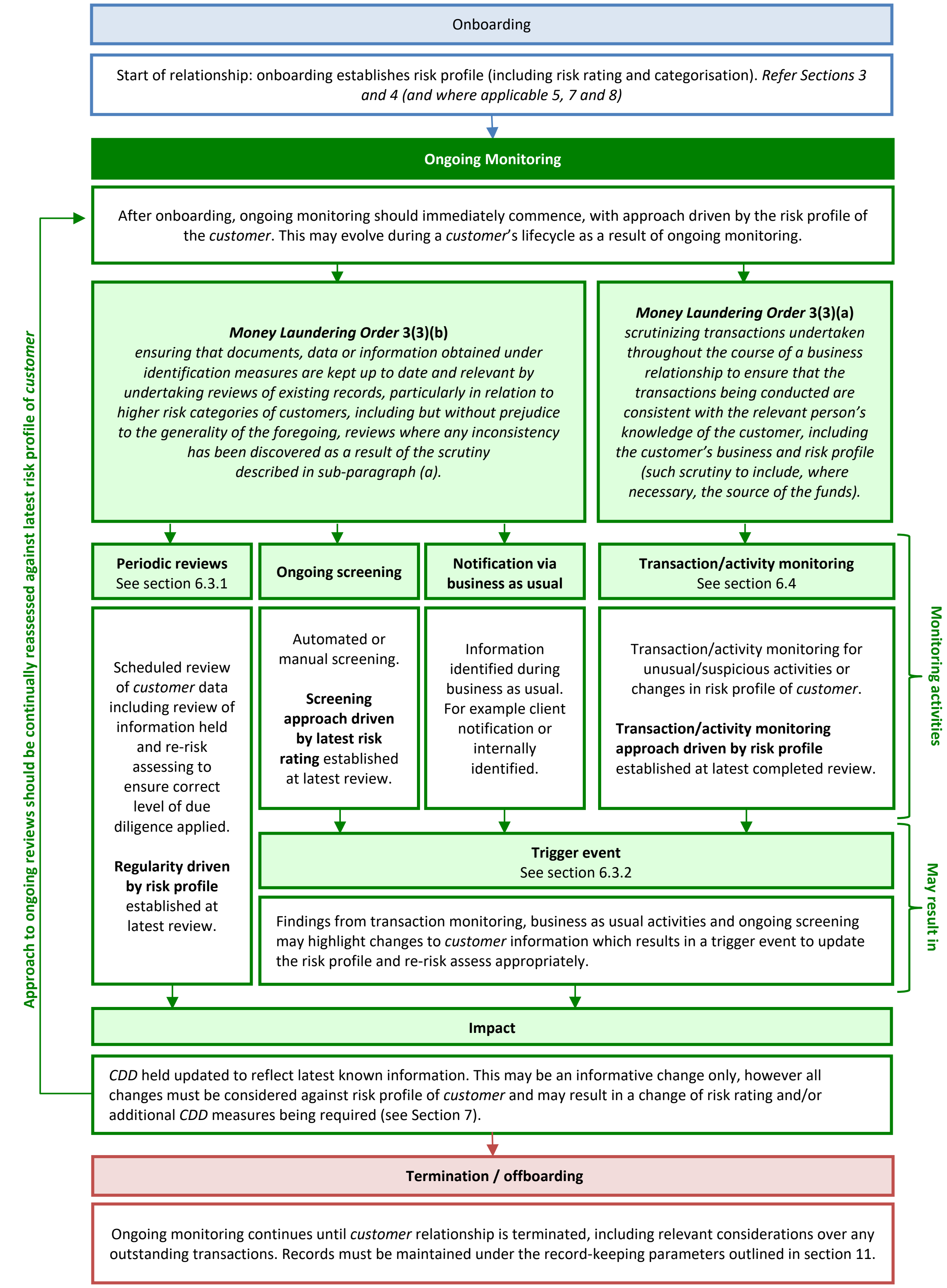
11. Monitoring may involve **manual** and **automated processes**. Automated monitoring processes may add value to manual processes by recognising transactions or activity that fall outside set parameters. This will be particularly so where a *supervised person* processes large volumes of *customer* transactions which are not subject to day-to-day oversight. However, where automated monitoring processes are not in place, monitoring is likely to be most effective when undertaken on a case-by-case basis by *customer* facing staff, administration, and accounts staff, whom may be expected to spot and highlight notable transactions or activity.

12. Where ongoing monitoring gives rise to a suspicion of *money laundering*, the *financing of terrorism*, or the *financing of proliferation* activity, an internal *SAR* must be made to the *MLRO*. Reporting of knowledge, suspicion, or reasonable grounds for knowledge or suspicion, of *money laundering*, the *financing of terrorism*, or the *financing of proliferation* is addressed in section 9 of *this Handbook*.

13. Practical guidance on financial sanctions implementation matters, including an explanation of reporting obligations under the *Sanctions and Asset-Freezing Law*, is provided on the *JFSC*'s website. See also section 9.8 of *this Handbook.*

6.3 Monitoring requirements over *customer* lifecycle

14. Process-flow illustrating *the customer lifecycle, including the* interrelation between key ongoing monitoring components.



15. Ongoing monitoring: ensuring that documents, data and information are up to date and remain relevant

Overview

16. Article 3(3)(b) of the *Money Laundering Order* explains that ongoing monitoring includes ensuring that documents, data, or information obtained under *identification measures* are kept up-to-date and relevant by undertaking reviews of existing records, particularly in relation to higher risk categories of *customers*, including reviews where any inconsistency has been disclosed because of scrutiny.

17. Among other things, where there is a change to information found out about the *customer*, the *customer* acts for a new third party, a new person purports to act for the *customer*, or the *customer* has a new *Beneficial owner and/or controller*, Article 13(1)(c)(ii) of the *Money Laundering Order* requires that the identity of that person is found out and evidence obtained.

Guidance notes

6.3.1 Scheduled periodic reviews

18. A *supervised person* may demonstrate that documents, data and information obtained under *identification measures* are kept up-to-date and relevant under Article 3(3)(b) of the *Money Laundering Order* where they are reviewed on a risk-sensitive basis, including where additional “factors to consider” (see section 3) or trigger events occur which may impact the *customer* business and risk profile.

19. A *supervised person* may demonstrate that documents, data or information obtained under *identification measures* are kept up-to-date and relevant under Article 3(3)(b) of the *Money Laundering Order* where the *customer* is requested to, and does provide, an assurance that they will update the information provided on a timely basis in the event of a subsequent change.

20. The frequency of scheduled periodic reviews should be based on the risk rating of the *customer* as set out in the *customer* risk assessment. *Supervised persons* are expected to record the frequency of periodic reviews aligned to the relevant risk profiles in their policies and procedures. Higher risk categories of *customer*s, particularly (as indicated by Article 3(3) (b) of the *MLO)* may require more frequent and detailed reviews, see also section 6.4 for enhanced ongoing monitoring.

6.3.2 Trigger events

21. A trigger event is an event or circumstance that triggers the *supervised person* to review the information and documentation held on the customer to ensure that it is comprehensive, accurate and up to date.

22. Trigger events may also present a convenient opportunity to reassess the *customer*’s risk profile and review documents, data and information obtained under *identification measures*. Such review may result in the *customer*’s risk profile changing, enhanced due diligence becoming necessary or the filing of a suspicious activity report.

23. Non exhaustive examples of potential trigger events:

- Customer advises of change of circumstances as per terms of engagement e.g. change of domicile, change to the family
- Automated database screening raises an alert, e.g. indicates *customer* has become a PEP or connected to a PEP
- Adverse media on *customer* or persons connected to the *customer*

› Doubts about currentness of *customer* information	› Change of intermediary who acts on behalf of *customer* and provides instructions	› JFSC examination findings flags ongoing monitoring common failings
› Customer purchases further product or opens a new account	› Meeting with *customer* to discuss new business	› Awareness *customer* is having financial difficulties
› Unusual transactions	› Update to Appendix D2	› Court case outcome
› Change to customer's Source of Wealth and/ or changes in risk profile of customer's SoW	› Material changes to the assets and business activities of a structure and exclusion/addition of beneficiaries to a Trust	› Change to *customer*'s risk profile
› New taxation reporting requirements	› Change in corporate form of *customer* e.g. merger	› Change in *customer*'s ownership and control structure
› Undeliverable post	› Change to *customer*'s Source of Funds	› Update to Sanctions list
› Scrutiny of transactions reveals inconsistency	› Controller through other means identified	› Employee suspicion of ML/TF/PF arises regarding *customer*

6.4 Ongoing monitoring: transactions and activity

Statutory requirements (paraphrased wording)

24. *Article 11 of the Money Laundering Order requires a relevant person to maintain appropriate and consistent policies and procedures for the application of CDD measures, having regard to the degree of risk of money laundering and the financing of terrorism. The policies and procedures referred to include those:*

- *which provide for the identification and scrutiny of:*
  - *complex or unusually large transactions;*
  - *unusual patterns of transactions, which have no apparent economic or visible lawful purpose; or*
  - *any other activity which the relevant person regards as particularly likely by its nature to be related to money laundering or the financing of terrorism.*
- *which determine whether:*

  a. business relationships or transactions are with a person connected with a country or territory in relation to which the FATF has called for the application of enhanced CDD measures; or

  b. business relationships or transactions are with a person:

    i. subject to measures under law applicable in Jersey for the prevention and detection of money laundering;

    ii. connected with an organization that is subject to such measures; or

    iii. connected with a country or territory that is subject to such measures.

25. *Article 11(3A) of the Money Laundering Order explains that, for the purposes of Article 11(3)(a), "scrutiny" includes scrutinising the background and purpose of transactions and activities.*

26. *Parts 3, 4 and 5 of the Sanctions and Asset-Freezing Law set out a range of restrictions and prohibitions in respect of designated persons. These relate to funds, economic resources and financial services.*

27. *By virtue of the Sanctions and Asset-Freezing Law, UK designations have immediate effect in Jersey.*

28. *Article 32(1) of the Sanctions and Asset-Freezing Law requires a relevant financial institution to inform the Minister for External Relations and Financial Services (the Minister) as soon as practicable if:*

- *it holds an account of a person, has entered into dealings or an agreement with a person or has been approached by or on behalf of a person;*
- *it knows, or has reasonable cause to suspect, that the person:*
    - *is a designated person; or*
    - *has committed, is committing, or intends to commit an offence under that law; and*
- *the information or other matter on which the knowledge or reasonable cause for suspicion is based came to it in the course of carrying on its business.*

AML/CFT/CPF Codes of Practice

[COP58] In addition to the scrutiny of transactions, ongoing monitoring must also involve scrutinising activity in respect of a business relationship to ensure that the activity is consistent with the *supervised person*'s knowledge of the *customer*, including the *customer*'s business and risk profile.

[COP59] A *supervised person* must establish and maintain appropriate and consistent *policies and procedures* which provide for the **identification** and **scrutiny** of:

- complex or unusually large activity;
- unusual patterns of activity, which have no apparent economic or visible lawful purpose; and
- any other activity, the nature of which causes the *supervised person* to regard it as particularly likely to be related to *money laundering*, the *financing of terrorism*, or the financing of proliferation.

[COP60] As part of its examination of the above transactions, a *supervised person* must **examine**, as far as possible, their background and purpose and set forth its findings in writing.

Guidance notes

6.4.1 Scrutiny of transactions and activity

29. High level approach to the three pillars of transaction and activity monitoring described below.

1

Supervised person defines expected transaction/activity profile of *customer*

30. Transaction monitoring should be established through onboarding and subsequent ongoing monitoring, taking into account risk profile of *customer* with factors such as (but not limited to) risk rating, expected turnover/transactions, geographic sphere of activities, industry and products to establish expected transaction/activity profile.

31. Sections 3 and 4 of *this Handbook* address the capturing of sufficient information about a *customer*, allowing a *supervised person* to record a ***customer* business and risk profile** which provides a basis for recognising notable transactions/activity, which may indicate *money laundering*, the *financing of terrorism*, or the *financing of proliferation*.

32. Where a *supervised person's customer* base is homogeneous, and where the products and services provided to *customer*s result in uniform patterns of transactions or activity, it may be easier to establish parameters to identify usual transactions/activity. For example, when dealing with local property transactions being passed before the Royal Court or undertaking deposit taking activities.

33. Where each *customer* is unique, and where the product or service is bespoke, a *supervised person* will need to tailor monitoring systems to the nature of its business and facilitate the application of additional judgement and experience to the recognition of unusual transactions and activity. This is particularly the case when transactions are being made in VAs.

34. Higher risk or complex transactions/activity may be recognised by developing a set of 'red flags' or indicators which may indicate *money laundering*, the *financing of terrorism*, or the financing of proliferation, based on a *supervised person's* understanding of its business, products and *customer*s (i.e. the outcome of its BRA – section 2.3.1 of *this Handbook*).

2

Supervised person monitors all transactions and activity

35. Based on expectations outlined in step 1, *supervised person* monitors all transactions and activity to recognise notable transactions or activity that:

› are inconsistent with the *supervised person's* knowledge of the *customer* (including inconsistency with the normal business activities for the product/service being offered);
› are complex or unusually large;
› form part of an unusual pattern; or
› present a higher risk of *money laundering*, the *financing of terrorism*, or the financing of proliferation.

36. A *supervised person* must therefore, as a part of its scrutiny of transactions/activity, establish appropriate procedures to monitor all its *customers*' transactions/activity, and to recognise and examine notable transactions/activity.

37. Scrutiny may involve both real time and post event monitoring. Real time monitoring will focus on transactions and activity when information or instructions are received from a *customer*, before or as the instruction is processed. Post event monitoring may involve end of day, weekly, monthly or annual reviews of *customer* transactions and activity. Real time monitoring of transactions and activity will more effectively reduce a *supervised person's* exposure to *money laundering*, the *financing of terrorism*, and the financing of proliferation. Post event monitoring may be more effective at identifying unusual patterns.

3

Appropriate person reviews transactions identified and takes necessary steps

38. Where notable transactions or activity are **recognised**, they will need to be **examined**. The purpose of this examination is to determine whether there is an **apparent economic** or **visible lawful purpose** for the transactions or activity. It is not necessary (nor will it be possible) to conclude with certainty that a transaction or activity has an economic or lawful purpose. Sometimes, it may be possible to make such a determination based on an existing *customer* business and risk profile and on occasion this examination will involve requesting additional information from a *customer*.

39. Such notable transactions and activity, including their background and purpose, should be examined by an appropriate person to ensure that they are within:

› the expected pattern of transactions;
› the expected activity for a particular *customer*; or
› the normal business activities for the type of product or service that is being delivered.

40. Notable transactions or activity may indicate *money laundering*, the *financing of terrorism*, or the *financing of proliferation* where there is no apparent economic or visible lawful purpose for the transaction or activity, i.e., they are no longer just unusual but may also be suspicious. **Reporting** of knowledge, suspicion, or reasonable grounds for knowledge or suspicion of *money laundering* or the *financing of terrorism* or *proliferation financing* is addressed in section 9 of *this Handbook*.

41. Subsequent to the review, appropriate steps may need to be taken, which can include (but not be limited to) the following:

› An update of risk profile to ensure the latest *customer* information is maintained (see Trigger Events in Section 6.3.2);
› This may also impact the risk assessment, subsequent risk rating and risk categorisation of a *customer*, which could consequently require additional due diligence to be collected, and future ongoing monitoring approach may change (see Section 6.5 on *Enhanced Monitoring*);
› The raising of a Suspicious Activity Report (see Section 9.3);
› Further enquiries from the *customer* (if not constituting 'Tipping Off', see section 9.5);
› A cessation of activity and business with the *customer*.

42. The examination of notable transactions or activity may also be conducted either by *customer* facing employees, or by an independent reviewer. In any case, the examiner must have access to all *customer* records and be appropriately trained and experienced.

43. The results of an examination should be recorded, including appropriate action taken and rationale. Refer to section 11 of *this Handbook* for record-keeping requirements in relation to the examination of notable transactions and activity.

44. In addition to the scrutiny of **transactions** as required by the *Money Laundering Order*, *AML/CFT/CPF Codes of Practice* in this section also require a *supervised person* to scrutinise *customer* **activity**. This is not just relevant to transaction-based *business relationships*, but also to *business relationships* that do not involve transactions, e.g., where a *supervised person* gives investment advice, or acts as a director to a company.

45. Monitoring activities are required over all *customer*s to an extent that is appropriate for their risk profile. Additional or more frequent monitoring is required for relationships that have been designated as carrying a higher risk of *money laundering*, the *financing of terrorism*, or the *financing of proliferation (*enhanced monitoring as part of *enhanced CDD measures,* see section 6.6 below*)*.

46. External data sources and media reports may also assist with the identification of notable transactions and activity.

47. To **recognise** *money laundering*, the *financing of terrorism*, and the *financing of proliferation, employees* will need to have a good level of awareness of each, and to have received training. Refer to section 10 of *this Handbook* for raising awareness and training.

Guidance notes

48. A *supervised person* may demonstrate that *CDD policies and procedures* are appropriate where **scrutiny** of transactions and activity has regard to the following factors:

› its *BRA* (including the size and complexity of its business);

› the nature of its business and services;

› whether it is practicable to monitor transactions or activity in real time (i.e., before *customer* instructions are put into effect);

› whether it is possible to establish appropriate standardised parameters for automated monitoring; and

› the monitoring procedures that already exist to satisfy other business needs.

49. A *supervised person* may demonstrate that *CDD policies and procedures* are appropriate where the following are used to **recognise** notable transactions or activity:

› *customer* business and risk profile – see section 3.3.5 of *this Handbook*;

› ‘red flags’ or indicators of higher risk – that reflect the risk that is present in the *supervised person’s customer* base – based on its *BRA* (refer to section 2.3.1 of *this Handbook*), information published from time-to-time by the *JFSC* or *FIU*, e.g., findings of supervisory and themed examinations and typologies, and information published by reliable and independent third parties;

› ‘red flags’ or indicators of complex transactions and activity – based on its *BRA* (refer to section 2.3.1 of *this Handbook*), information published from time-to-time by the *JFSC* or *FIU*, e.g. findings of supervisory and themed examinations and typologies, and information published by reliable and independent third parties; and

› ‘red flags’ or indicators of sanctions evasion - based on its *BRA* (refer to section 2.3.1 of *this Handbook*), information published from time-to-time by the *JFSC* or the Government of Jersey, e.g. findings of supervisory/themed examinations and typologies, and information published by reliable and independent third parties.

50. A *supervised person* may demonstrate that *CDD policies and procedures* are appropriate if **examination** of notable transactions or activity includes:

› reference to the *customer’s* business and risk profile;

› as far as possible, a review of the background and purpose of a transaction or activity (set in the context of the business and risk profile); and

› where necessary, the collection of further information needed to determine whether a transaction or activity has an **apparent economic** or **visible lawful purpose**.

Case study:

› a *supervised person* may have a *business relationship* with a *customer* who previously advised that they had a modest *source of funds*.

› the *customer* then instructs the *supervised person* to purchase an asset, the value of which appears to be outside the means of the *customer’s source of funds,* as currently understood.

› while the *supervised person* may be satisfied that it still knows the identity of the *customer*, as part of its ongoing monitoring obligations, it would be appropriate to ask about the *source of funds* for this purchase. Depending on the *customer’s* willingness to provide such information, and the answer that is provided, the *supervised person's staff* should also consider whether they:

- are satisfied with the response;
- want further proof of the *source of funds*; and/or
- need to submit an internal *SAR* to the *supervised person's MLRO*.

51. A *supervised person* may demonstrate that *CDD* and reporting *policies and procedures* are effective if, **post-examination** of notable transactions or activity, it:

- revises, as necessary, its *customer's* business and risk profile;
- adjusts, as necessary, its monitoring system, e.g., it refines monitoring parameters, enhances controls for more vulnerable products/services/business units;
- considers if it knows, or has reasonable cause to suspect, that a person:
  - i) is a *designated person*; or
  - ii) has committed, is committing or intends to commit and offence under the *Sanctions and Asset-Freezing Law*; and
- considers whether it knows, suspects, or has reasonable grounds for knowing or suspecting that another person is engaged in *money laundering,* the *financing of terrorism*, or the *financing of proliferation*, or that any property constitutes or represents:
  - i) the proceeds of criminal conduct; or
  - ii) property used in or intended to be used in criminal conduct.

If the above applies, a suspicious activity report should be considered (refer to section 9)

6.5 Enhanced ongoing monitoring

52. A *supervised person* may demonstrate that it has applied enhanced ongoing monitoring to a higher risk *customer* where it:

- reviews the *business relationship* on at least an annual basis, including all documents, data and information obtained under *identification measures* in order to ensure that they are kept up-to-date and relevant. The document review should always include the obtaining of documentary/corroborating evidence to verify *source of funds* and *source of wealth* (where evidence is lacking) and updating beneficial ownership information.
- where monitoring thresholds are used, sets lower thresholds for transactions connected with the *business relationship*.

53. Additional or more frequent monitoring for relationships that have been designated as carrying a higher risk of *money laundering*, the *financing of terrorism*, or the financing of proliferation. Enhanced ongoing monitoring on a risk sensitive basis may be specifically required by statute, for example, Article 15A (2) of the *Money Laundering Order* in relation to:

- Business relationships/one of transactions with foreign PEPs and their immediate family members and close associates; and
- higher risk relationships/one off transactions with domestic PEPs or prominent persons or their immediate family members and close associate. See Section 7.6.

54. The *supervised person* may need to continue to assess the monitoring approach for suitability. A *customer* may require enhanced monitoring as a result of previous monitoring which impacts the *customer* risk profile.

6.5.1 Case studies

55. New accounts were being approved by senior management before screening was completed. In one case this resulted in the *customer* being identified as a politically exposed person after the account was opened.

56. Source of Wealth and Source of Funds records did not meet the *supervised person*'s requirements as outlined in their policies and procedures, for example, incorrect recording of the origins of Source of Wealth and Source of Funds and confusion as to what each term means. **Good Practice:** Source of Wealth and Source of Funds should be clearly defined in policies and procedures and be well understood by employees in *customer* facing roles and those employees tasked with *customer* onboarding and *customer* periodic reviews.

6.5.2 Existing Customers

57. Historically, Article 13(2) of the *Money Laundering Order* allowed for deferral of *CDD* measures, specifically finding out the identity of an existing *customer* (also known as legacy *customers*) with a relationship established before the *supervised person* was subject to *AML/CFT/CPF* requirements, subject to certain conditions. This concession became time barred on 31 December 2014 unless consent was sought from the JFSC. No such consents remain outstanding and therefore all existing *customers* should have been remediated. Article 13(1)(c)(ii) of the *Money Laundering Order* will apply to such a relationship in the same way as a relationship established on or after the dates referred to in Article above, on the basis that documents, data or information on all existing/legacy *customers* should align with the *CDD* measures prescribed in Article 3.

58. All existing/legacy *customers* are subject to ongoing monitoring and review of *CDD* information and evidence. The requirement to review *CDD* is not limited to high-risk *customers*.

59. Higher risk existing/legacy *customers* will be subject to the same programme of enhanced monitoring as any new high-risk *customer*.

6.5.3 Monitoring and recognition of *business relationships* and transactions – *Enhanced risk states* and targets subject to sanctions (e.g. a country or a *designated person*)

Overview

60. The risk that a *business relationship* is tainted by funds that are the proceeds of criminal conduct or instrumentalities, or are used to *finance terrorism* or the *financing of proliferation*, is increased where the *business relationship* or *one-off transaction* is with a person or entity connected with:

- an *enhanced risk state* (see **Appendix D1** of *this Handbook*);
- a *sanctioned country or territory* (see **Appendix D2** of *this Handbook*, sources 6 and 12 therein); or
- a *sanctioned person*.

61. A *supervised person* is required to comply with asset-freezing and reporting obligations to prevent funds or other assets being made available, directly or indirectly, for the benefit of a *designated person*. Changes to *UN and UK* asset-freeze designations are immediately effective in Jersey by virtue of the ambulatory provisions in Jersey's sanctions legislation.

62. *FATF Recommendations 6 and 7* require implementation of *UN TFS* "without delay", which should be understood as no more than 24 hours and interpreted in the context of:

- the need to prevent the flight or dissipation of funds or other assets which are linked to the *financing of terrorists* or *financing of proliferation* of weapons of mass destruction; and
- the need for global, concerted action to swiftly prevent and disrupt their flow.

63. Following changes to the sanctions designations lists effective in Jersey, the Government of Jersey will issue a sanctions notice without delay, and the *JFSC* will alert *supervised persons* of the changes.

64. As a part of its ongoing monitoring procedures, a *supervised person* must establish and maintain appropriate *policies and procedures* to **monitor** all *customer* transactions and activity to **recognise** whether any *business relationships* or *one-off transactions* are directly or indirectly with such *sanctioned person*s, organisations, or other parties.

65. There is not a separate requirement to **examine**, or have *policies and procedures* in place to examine, *business relationships* with an *enhanced risk state* once they are recognised. This is because *enhanced CDD measures* are required to be applied in line with Article 15(1)(c) of the *Money Laundering Order*. See section 7.5 of *this Handbook*.

66. There is not a statutory requirement to **examine**, or have *policies and procedures* in place to examine, *business relationships* or *one-off transactions* with a *designated person* once they are recognised. This is because provisions in financial sanctions legislation must be followed. Among other things, such provisions prohibit dealing with the assets of designated persons, and not making funds, economic resources, or financial services available to them. Further guidance is published on the *JFSC's* website and the Government of Jersey website.

AML/CFT/CPF Codes of Practice

[COP61] Ongoing monitoring must involve **examining** transactions and activity recognised as being with a person connected with an *enhanced risk state.*

[COP62] A *supervised person* must establish and maintain appropriate and consistent *policies and procedures* which provide for the **examination** of transactions and activity recognised as being with a person connected with an *enhanced risk state*.

[COP63] As part of its **examination** of the above transactions and activity, a *supervised person* must examine, as far as possible, their background and purpose and set forth its findings in writing.

[COP64] A *supervised person* must undertake sanctions screening for all *business relationships* and *one-off transactions*. This screening must include the *customer*, any *Beneficial owners and/or controllers* and other associated parties. The screening must be carried out at the time of take-on, periodic review and when there is a trigger event, i.e., amendments made to the sanctions designations lists.

[COP65] A *supervised person* must sign up to receive sanctions e-mail alerts from the *JFSC* and sanctions notices from the Government of Jersey, which are publicly available on the Jersey Gazette – see the Government of Jersey Sanctions Notices Registration (gov.je) and the *JFSC* Sanctions Registration (jerseyfsc.org).

[COP66] A *supervised person* must ensure their sanctions monitoring arrangements include an assessment of the effectiveness of their sanctions controls and their compliance with the Jersey sanctions regime.

Guidance notes

67. A *supervised person* may demonstrate that *CDD policies and procedures* are appropriate where **scrutiny** of transactions and activity has regard to the following factors:

› its *BRA* (including the size and complexity of its business and risks arising from breach, non-implementation or evasion of sanctions obligations);

› the nature of its business and services;

› whether it is practicable to monitor transactions or activity in real time (i.e., before *customer* instructions are put into effect);

› whether it is possible to establish appropriate standardised parameters for automated monitoring; and

› the monitoring procedures that already exist to satisfy other business needs.

68. A *supervised person* may demonstrate that *CDD policies and procedures* are appropriate where the following are used to **recognise** connections with *enhanced risk states*, *sanctioned countries and territories*, *sanctioned persons,* and how sanctions measures may impact the *supervised persons* business:

› all *customers* – Business and risk profile in line with section 3.3.5 of *this Handbook*;

› all *customers* – Adopting the sanctions designations lists as a comprehensive listing of designated persons subject to sanctions measures applicable in Jersey;

› all *customers* – Considering methods of identifying possible indirect associations and connections (also referred to as 'indirect links') that may exist between the *supervised person's customer* and any *sanctioned persons* and/or *enhanced risk states*, that will not immediately be obvious from screening of the relevant sanctions designations lists;

› *enhanced risk states* - **Appendix D1** of *this Handbook*; and

› sanctioned countries and territories - **Appendix D2** of *this Handbook* (sources 6 and 12 therein).

› sanctions measures- there are many types of sanctions measures which will need to be kept under review and consideration given as to how these may impact the supervised persons business, for example prohibitions on providing particular services or engaging in specific transactions under certain sanctions regimes.

Statutory requirements (paraphrased wording)

69. Under Article 2A of the Sanctions and Asset-Freezing (Jersey) Law 2019 provides guidance on when an account, funds or economic resources are owned indirectly and Schedule 2 set out rules of interpretation.

70. If someone owns or controls funds or resources jointly with others, they are still treated as owning or controlling them.

71. "Indirect ownership or control" means:

› Another person holds the asset but acts as your employee, agent, nominee, or under your direction or on your behalf.

› There is an arrangement where it's reasonable to believe they will act according to your wishes or with your consent.

72. For companies or other legal entities:

› You control them if you own more than 50% of shares or voting rights, or can appoint/remove most of the board.

› Even without those rights, if you can generally make the company follow your wishes, you are considered to control it.

73. Control can flow through chains of ownership — if you control Company A, and Company A controls Company B, you are treated as controlling Company B.

74. Schedule 2 explains how to calculate indirect control:

› Shares or rights held by nominees or through arrangements count as yours.

› Rights you can exercise only in certain circumstances still count if those circumstances exist.

› Rights held as security may count if you can exercise them.

› Joint arrangements and agreements to act together can combine holdings.

› Control can be inferred from influence, not just formal rights.

75. Indirect links as described in the above paragraph may be formed through any relationship between the *customer* and its close associates including, but not limited to, political links, financial links, familial links, social links, professional links and business (e.g. *customer*s and suppliers) links.

76. A *supervised person* may look to mitigate risks of undetected indirect links by considering:

› Have all reasonable steps been taken to ascertain close associates and family ties (examples described under 7.6.1)to identify potential sanctions evasion and do your policies and procedures ensure that these have been appropriately investigated and documented?

› Has sufficient scrutiny been applied to establish any additional indirect links who may have influence (as outlined in above paragraph)?

› Have all connections identified in the above two steps been screened at the point of onboarding?

› Is ongoing screening sufficiently regular to detect any changes in circumstance given the profiles of those subject to screening?

› Is the configuration of screening (both at onboarding and ongoing) appropriate given the profile of those being screened (e.g. adverse media results, screening results, the risk profile associated with them, the countries in which they operate, the industries in which they operate and the known links they presently hold) to detect changes in information in relation to indirect links that may occur during the relationship with that *customer*? It may be that entities overnight screening/data analytics are configured to identify customers who may be close associates or dependents or have transactional links with designated persons, and so may represent a higher risk of sanctions non-compliance.

77. Sanctions are not static. Supervised person as good practice may wish to consider scenarios where sanctions breaches may occur and test/consider whether your sanctions screening is robust enough to flag sanctions issues. For example, the following scenarios where there are indirect sanctions links which have been identified by an administrator's screening measures:

- A request is received from an individual who is based in a jurisdiction where some of the residents are subject to financial sanctions. The individual asks for a third-party payment to be made, with the third party being a friend or colleague of the individual. The individual is on a sanctions list, and this is picked up by the administrator who screens third party payments.
- Two individuals are majority shareholders of a company, one of them being a sanctioned individual. This is a new sanction listing and has been identified by the administrator via overnight screening.
- During the course of a business relationship, it is identified that an individual who is the UBO/Settlor/Founder (i.e. funder of a structure) provides services to sanctioned individuals via other business interests. During a periodic review higher risk connections have been flagged and following further manual investigations these connections have been discovered by the administrator.
- A wealthy individual goes through the CDD process, they reside in a jurisdiction that is not high risk, their source of wealth and funds is verified. A trust is set up for the individual and used to purchase its main asset which is an expensive mansion. During an administrators overnight screening he is flagged as having social and business dealings with an oligarch who is sanctioned. Following their policies and procedures this flag is reviewed by the compliance team who determine that further enquiries are required. These further enquiries yield information that the mansion owned by the wealthy individual via his jersey trust is being used as a residential address by the sanctioned oligarch.

78. A *supervised person* should have appropriate *systems and controls* (including *policies and procedures*) in place to ensure that a change to the *UK* and *UN* sanctions designations lists is reviewed and acted upon "without delay". This term is defined in *FATF*'s Best Practices Paper: Targeted Financial Sanctions Related to Terrorism and Terrorist Financing Recommendation 6, on page 9, as meaning "ideally, within a matter of hours of a designation". This activity should include a comparison of the *supervised person's customer* base against the *designated persons* listed within the sanctions notices.

79. *A supervised person* is encouraged to refer to the *FSIU's guidance* in terms of the *supervised person's* unfreezing procedure.

80. A *supervised person* may demonstrate that *CDD policies and procedures* are appropriate if **examination** of transactions or activity recognised as being with a person connected with an *enhanced risk state* includes:

› reference to the *customer's* business and risk profile;

› as far as possible, a review of the background and purpose of a transaction or activity (set in the context of the business and risk profile); and

› where necessary, the collection of further information needed to determine whether a transaction or activity has an **apparent economic** or **visible lawful** purpose.

81. A *supervised person* may demonstrate that *CDD* and reporting *policies and procedures* are appropriate if post-examination of transactions or activity recognised as being with a person connected with an *enhanced risk state* it:

- revises, as necessary, its *customer's* business and risk profile;
- adjusts, as necessary, its monitoring system e.g., refines monitoring parameters, enhances controls for more vulnerable products/services/business units;
- considers if it knows, or has reasonable cause to suspect, that a person:
  - i) is a *designated person*; or
  - ii) has committed, is committing or intends to commit and offence under the *Sanctions and Asset-Freezing Law;* and
- considers whether it knows, suspects, or has reasonable grounds for knowing or suspecting that another person is engaged in *money laundering*, the *financing of terrorism*, or the *financing of proliferation*, or that any property constitutes or represents:
  - i) the proceeds of criminal conduct; or
  - ii) property used in or intended to be used in criminal conduct.

82. Examples of effective sanctions compliance include, but are not limited to:

- having appropriate procedures in place to ensure that the content of targeted financial sanctions amendments is reviewed **without delay**, including screening of *customer* data against the sanctions designations lists;
- in the case of an identified positive match, freezing of such accounts, and other funds or economic resources without notice and without delay;
- refraining from dealing with the funds or assets or making them available (directly or indirectly) to such persons unless licensed by the *Minister;*
- sanctions compliance reports required under the *Sanctions and Asset-Freezing Law* are filed as soon as practicable.
- identifying where there is an accumulation of risks i.e. nexus to a sanctioned country and higher risk activities, for example to manage the risk where funds flowing up a trust structure from its non TCB managed trading companies due to an underlying asset undertaking sanctioned activities or facilitating sanctioned activities, such as mining in an appendix D2 country

83. A *supervised person* may wish to undertake their assessment of effectiveness as part of their compliance monitoring plan activities. The assessment may be presented to the board in the form of a report by the *MLCO*.

84. In the context of sanctions compliance reports, "as soon as practicable" means as soon as possible and practical, considering all of the facts and circumstances in the individual case. For example key facts should be reported within 24/48 hours with a more detailed report to follow later, if appropriate. Obtaining independent legal advice may delay immediate reporting of a sanctions matter and take some time, however, it is reasonable to suggest that the issue will be resolved within a matter of days. In any case, this should be no more than 14 days.

85. Further examples of good practice in respect of a range of sanctions compliance matters can be found in the *JFSC's* Financial sanctions practical guidance and the Government of Jersey website.

6.6 Automated monitoring methods

Overview

86. Automated monitoring methods may be effective in recognising notable transactions and activity, and *business relationships* and *one-off transactions* with persons connected to *enhanced risk states, sanctioned countries or territories*, or *sanctioned persons*.

87. **Exception reports** can provide a simple but effective means of monitoring all transactions to, or from, particular geographical locations or accounts, and any activity that falls outside of pre-determined parameters, based on thresholds that reflect a *customer*'s business and risk profile.

88. Large or more complex *supervised persons* may also use automated monitoring methods to facilitate the monitoring of significant volumes of transactions, or – such as in an e-commerce environment – where the opportunity for human scrutiny of individual transactions is limited.

89. What constitutes unusual behaviour by a *customer* is often defined by the automated monitoring system selected by the *supervised person*. It is important that the system selected has an appropriate definition of 'unusual' and is in line with the nature of business conducted by the *supervised person*.

90. Where an automated monitoring method (group or otherwise) is used, a *supervised person* will need to understand:

› how the system works and when it is changed;

› its coverage (who or what is monitored and what external data sources are used);

› how to use the system, e.g., making full use of guidance; and

› the nature of its output (exceptions, alerts etc.).

91. Use of automated monitoring methods does not remove the need for a *supervised person* to otherwise remain vigilant. Factors such as staff intuition, direct contact with a *customer* and the ability, through experience, to recognise transactions and activity that do not seem to make sense, cannot be automated.

92. In the case of **screening** of a *business relationship* (before establishing that relationship and subsequently) and transactions, the use of electronic external data sources to screen *customers* may be particularly effective. However, where a *supervised person* uses group screening arrangements, it will need to be satisfied that it provides adequate mitigation of risks applicable to the Jersey business. In all cases, it is important that a *supervised person*:

› understands which *business relationships* and transaction types are screened;

› understands the system's capacity for **fuzzy matching** (a technique used to recognise names that do not precisely match a target name, but which are still potentially relevant);

› sets clear procedures for dealing with potential matches, driven by risk considerations rather than resources; and

› records the basis for **discounting** alerts (e.g., false positives) to provide an audit trail.

93. The audit trail should enable a *supervised person* to review the dates on which screening checks were undertaken and the results of those checks (e.g., the number of false positives), thus allowing them to assess if the system is operating effectively. Where the *supervised person* is part of a wider group and utilises a group-wide screening system, a written confirmation from its head office may be obtained which confirms that such an audit trail exists and that its records can be accessed upon request.

94. By way of example, **fuzzy matching** arrangements can be used to identify the following variations:

Variation	Example

Different spelling of names.	"Jon" instead of "John". "Abdul" instead of "Abdel".
Name reversal.	"Adam, John Smith" instead of "Smith, John Adam".
Shortened names.	"Bill" instead of "William".
Insertion/removal of punctuation and spaces.	"Global Industries Inc" instead of "Global-Industries, Inc.".
Name variations.	"Chang" instead of "Jang".

95. Further information on screening practices may be found in reports published by the *JFSC* in August 2014, May 2021. Practical guidance in respect of financial sanctions is also available on the *JFSC*'s website.

6.7 *Money laundering* warning signs

Overview

96. Article 13 of the *Money Laundering Order* requires a *supervised person* to apply ongoing monitoring throughout the course of a *business relationship* and take steps to be aware of transactions with heightened *money laundering*, the *financing of terrorism*, and the *financing of proliferation* risks. The *Proceeds of Crime Law* requires a *supervised person* to report suspicious transactions and activity (see section 9 of *this Handbook*).

97. This section highlights several general warning signs for *supervised persons* to help them decide whether there may be reasons for concern, or the basis for a reportable suspicion.

98. In relation to ongoing monitoring, a *supervised person* should have regard both to the warning signs contained in the relevant sector-specific sections of *this Handbook* and the general indicators set out below, where they may become vulnerable to *money laundering*, the *financing of terrorism*, or the *financing of proliferation*. These warning signs apply to ongoing relationships just as much as to circumstances that may arise at the start of a *business relationship.*

99. Because *money launderers, terrorist financers*, and *proliferators of weapons of mass destruction* are always developing new techniques, no list of examples can be fully comprehensive. However, the following are some key factors indicating activity or transactions which might heighten a *customer*'s risk profile or give cause for concern.

6.7.1 Secretive *customers*

100. Whilst face-to-face contact with *customers* is not always possible, an excessively obstructive or secretive *customer* may be a cause for concern. Consideration should be given as to whether *customers* who demand strict confidentiality relating to their financial and business affairs, or are reluctant to answer *CDD* questions, are evading tax or seeking to mask the true beneficial ownership of their assets.

6.7.2 Unusual instructions

101. Instructions that are unusual in themselves, or that are unusual for the *supervised person,* or the *customer* may give rise to concern, particularly where no rational or logical explanation can be given. Be wary of:

- loss-making transactions where the loss is avoidable;

- dealing with money or property when there are suspicions that it is being transferred to avoid the attention of either a trust in a bankruptcy case, a revenue authority (e.g., *UK's* HM Revenue and Customs, Revenue Jersey etc.), or a law enforcement agency;
- complex or unusually large transactions, particularly where underlying *beneficial ownership* is difficult to ascertain and/or where the underlying transactions have been conducted in cash;
- unusual patterns of transactions which have no apparent economic purpose particularly those where a number of jurisdictions and different entities are involved for no logical business reason;
- funds that are being switched between investments or jurisdictions for no apparent reason;
- use of shell companies, blind trusts or other structures that are merely being used as a front for other activities;
- excessive use of off-balance sheet transactions or activity.

6.7.2.1 **Instructions outside the *supervised person's* area of expertise**

102. Taking on work which is outside the *supervised person's* normal range of expertise can present additional risks because a money launderer, terrorist financer or financier of proliferation of weapons of mass destruction might be using the *supervised person* to avoid answering too many questions. A *supervised person* inexperienced in the provision of a particular product or service might be influenced into taking steps which a more experienced business would not contemplate. *Supervised persons* should be wary of highly paid niche areas of work in which they have no background, but in which the *customer* claims to be an expert.

103. If the *customer* is not resident in Jersey, *supervised persons* should satisfy themselves that there is a genuine legitimate reason why they have been approached. For example, have the *supervised person's* services been recommended by another *customer*? Making these types of enquiries makes good business sense, as well as being a sensible *AML/CFT/CPF* check.

6.7.2.2 **Changing instructions**

104. Instructions that change unexpectedly or significantly might be suspicious, especially if there seems to be no logical reason for the changes. This may also be the case where the person making the instruction changes. The obligation to re-conduct *CDD* may well arise.

105. The following situations could give rise to cause for concern:

- a *customer* deposits funds into a *supervised person's* client account for a transaction, but then ends the transaction for no apparent reason;
- a *customer* advises that funds are coming from one source and at the last minute the source changes; and
- a *customer* unexpectedly requests that money received into a *supervised person's* client account be sent back to its source, to the *customer* or to a third party.

6.7.3 Use of client accounts

106. Client accounts should only be used to hold *customer* money for legitimate transactions for *customers*, or for another proper legal purpose. Putting criminal money through a *supervised person's* client account can make it appear clean, whether the money is sent back to the *customer*, on to a third party, or invested in some way. Introducing cash into the banking system can become part of the placement stage of *money laundering*. Therefore, the use of cash for non-cash-based businesses is often a warning sign/red flag.

6.7.3.1 ***Source of funds***

107. If funding is from a source other than the *customer*, *supervised person*s may need to make further enquiries, especially if the *customer* has not previously advised that a third party would be involved. When considering whether to accept funds from a third party, *supervised person*s should ask how and why the third party is helping with the funding.

108. A *supervised person* must always be alerted to warning signs and in some cases will need to seek more information.

6.7.4 *Money laundering* offences factors

6.7.4.1 **Intent**

109. Except for certain strict liability offences, criminal conduct requires an element of criminal intent which means that an offender must know or suspect that an action or property is criminal. Conduct which is an innocent error or mistake may be criminal where it constitutes a strict liability offence but will not also be *money laundering*.

110. If an individual or *supervised person* knows or believes that a *customer* is acting in error, the *customer* may be approached, and the situation and legal risks explained to them. However, once the criminality of the conduct is explained to the *customer*, they must bring their conduct (including past conduct) promptly within the legislation to avoid a *money laundering* offence being committed. Where there is uncertainty about the legal issues that are outside the competence of the *supervised person, customers* should be referred to an appropriate specialist or legal adviser.

111. If there are reasonable grounds to suspect that a *customer* knew or suspected that their actions were criminal, a report must be made. Even if the *customer* does not have the relevant intent, but the *supervised person* is aware that there is criminal property, consideration needs to be given to whether a report must be made to the *FIU*.

112. In all circumstances, *supervised person*s should be mindful of committing a 'tipping-off' offence as set out at Article 35(4) of the *Proceeds of Crime Law*. See section 9.5 of *this Handbook* for more information.

6.7.4.2 **Holding of funds**

113. *Supervised persons* who choose to hold funds on behalf of a *customer* should consider the checks to be made about the funds they intend to hold before the funds are received. Consideration should be given to conducting *CDD* measures on all those on whose behalf the funds are being held.

114. Consideration should be given to any proposal that funds are collected from a number of individuals whether for investment purposes or otherwise. This could lead to wide circulation of client account details and payments being received from unknown sources.

6.7.4.3 **Factors arising from action by the *customer* or its *controllers***

115. Where a *customer* is actively involved in *money laundering*, the signs may include:

- unusually complex corporate structure where complexity does not seem to be warranted, or cannot be explained;
- complex or unusual transactions, possibly with related parties;
- transactions with little commercial logic taking place in the normal course of business (such as selling and re-purchasing the same asset);
- transactions conducted outside of the normal course of business or where the method of payment/receipt is not usual business practice, such as wire transfers or payments in foreign currency;
- transactions where there is a lack of information or explanation, or where explanations are unsatisfactory;
- transactions that are under- or overvalued, including double billing;
- transactions with companies whose identity or beneficial ownership is difficult to establish;
- abnormally extensive or unusual related party transactions;
- unusual numbers of cash transactions for substantial amounts or a large number of small transactions that add up to a substantial amount;
- payment for unspecified services or for general consultancy services; and
- long delays in the production of company or trust accounts for no apparent reason.

6.7.4.4 **Where the *customer* may unknowingly be a party to *money laundering*, the *financing of terrorism*, or the *financing of proliferation.***

116. There may be occasions where **the *customer* has been duped by its own *customer*** into providing assistance or becoming a vehicle for *money laundering*, the *financing of terrorism*, or the *financing of proliferation*. Warning signs may be:

- unusual transactions without an explanation, or a pattern of trading with a *customer* of the *supervised person's customer* that is different from the norm;
- request for settlement of sales in cash;
- the *customer's customer* setting up a transaction that appears to be of no commercial advantage or logic;
- the *customer's customer* requesting special arrangements for vague purposes;
- unusual transactions with companies registered in other jurisdictions;
- request for settlement to bank accounts or jurisdictions which would be unusual for a normal commercial transaction; or
- excessive overpayment of accounts, subsequently requesting a refund.

6.7.5 Administration of estates

117. A deceased person's estate is very unlikely to be actively utilised by criminals as a means for laundering their funds; however, there is still a risk of *money laundering* for those working in this area.

118. When winding up an estate, there is no blanket requirement that *supervised persons* should be satisfied about the history of all the funds which make up the estate under administration. However, *supervised persons* should be aware of the factors which can increase *money laundering* risks and consider the following:

- where estate assets have been earned in a foreign jurisdiction, *supervised persons* should be aware of the wide definition of criminal conduct in Article 1 of the *Proceeds of Crime Law*; and
- where estate assets have been earned or are in a *higher risk country or territory*, *supervised persons* may need to make further checks about the source of those funds.

119. *Supervised persons* should be alert from the outset and monitor throughout so that any disclosure can be considered as soon as knowledge or suspicion is formed, and problems of delayed consent can be avoided.

120. *Supervised persons* should bear in mind that an estate may include criminal property. An extreme example would be where the *supervised person* knows or suspects that the deceased person was accused or convicted of acquisitive criminal conduct during their lifetime.

121. If *supervised persons* know or suspect that the deceased person improperly claimed welfare benefit or had evaded the due payment of tax during their lifetime, criminal property will be included in the estate and so a *money laundering* disclosure may be required.

122. Relevant local laws will apply before assets can be released. For example, a grant of probate will normally be required before *UK* assets can be released. *Supervised persons* should remain alert to warning signs, for example if the deceased or their business interests are based in a *higher risk country or territory*.

123. If the deceased person is from another jurisdiction and a Lawyer is dealing with the matter in the home country, *supervised person*s may find it helpful to ask the Lawyer for information about the deceased to gain some assurances that there are no suspicious circumstances surrounding the estate. The issue of the tax payable on the estate may depend on the jurisdiction concerned.

6.7.6 Charities

124. While most charities are used for legitimate reasons, they can be used as vehicles *for money laundering*, the *financing of terrorism*, or the *financing of proliferation*.

125. *Supervised persons* acting for charities should consider their purpose and the organisations they are aligned with. If money is being received on the charity's behalf from an individual or a company donor, or a bequest from an estate, *supervised persons* should be alert to unusual circumstances, such as receipt of unexpectedly large sums of money.

6.7.7 Taxation matters

126. There are several tax offences which can give rise to the proceeds of crime and therefore require the submission of a *SAR* to the *FIU*. A *supervised person* is not required to be an expert in criminal law, but they would be expected to recognise activity which might suggest the *customer* is involved in tax evasion.

127. There will, however, be no question of criminality where the *customer* has adopted in good faith, honestly and without misstatement, a technical position with which a revenue authority disagrees.

128. The main areas where offences may arise in relation to direct tax are:

› tax evasion, including making false returns (including supporting documents), accounts or financial statements or deliberate failure to submit returns and

› deliberate refusal to correct known errors.

6.7.7.1 **Innocent or negligent error**

129. Where a *customer* indicates that they are unwilling, or refuse, to disclose an innocent mistake or negligent act to the *competent authority* to avoid paying the tax due, the *customer* appears to have formed a criminal intent and therefore a reporting obligation arises. The *supervised person* should also consider whether they can continue to act for the *customer*. This paragraph applies equally to potential *customer*s for whom the *supervised person* has declined to act.

6.7.7.2 **Intention to underpay**

130. *Customer*s may suggest that they will, in the future, underpay tax. This would be tax evasion and a *money laundering* offence when it occurs. A *supervised person* should investigate whether the *customer* has understood their obligations under the relevant legislation. Should the *customer's* intention in this regard remain in doubt, the *supervised person* should consider carefully whether they can commence, or continue, to act, and if in doubt should seek specialist legal advice. A *SAR* may well be required in such cases.

6.7.8 Observation of unlawful conduct

131. It should be borne in mind that for property to be criminal property, not only must it constitute a person's benefit from criminal conduct, but the alleged offender must know or suspect that the property constitutes such a benefit. This means, for example, that if someone has made an innocent error, even if such an error resulted in benefit and constituted a strict liability criminal offence, then the proceeds are not criminal property, and no *money laundering* offence has arisen until the offender becomes aware of the error.

132. Examples of unlawful behaviour which may be observed, but which are not reportable as *money laundering*, are set out below:

› offences where no proceeds or benefit results, such as the late filing of company accounts. However, *supervised persons* should be alert to the possibility that persistent failure to file accounts could represent part of a larger offence with proceeds, such as fraudulent trading or credit fraud involving the concealment of a poor financial position;

› misstatements in tax returns, for whatever cause, but which are corrected before the date when the tax becomes due;

› attempted fraud where the attempt has failed and so no benefit has accrued (although this may still be an offence in some jurisdictions e.g., the *UK*); andwhere a *customer* refuses to correct, or unreasonably delays in correcting, an innocent error that gave rise to proceeds and which was unlawful, firms should consider what that indicates about the client's intent and whether the property has now become criminal property.

7 *ENHANCED CDD MEASURES*

7.1 Overview of section

1. This section explains the circumstances in which *CDD* measures are required to be enhanced under Articles 15, 15A and 15B of the *Money Laundering Order* and explains the exemptions from CDD requirements under Part 3A of the *Money Laundering Order*. It also sets out circumstances where simplified *identification measures* can be applied in relation to low-risk products or services.

2. In addition to any case where a *supervised person* determines that a *customer* presents a higher risk of *money laundering*, the *financing of terrorism*, or *proliferation financing*, Articles 15, 15A and 15B of the *Money Laundering Order* also require *enhanced CDD* measures to be applied in the following specified scenarios:

- *customer*, or some other person, is not physically present for identification purposes – section 7.4 of this Handbook;
- *customer* has a relevant connection to an enhanced risk state – section 7.5 of this Handbook;
- *customer*, or some other prescribed person, is a PEP – section 7.6 of this Handbook;
- *customer* is a non-resident – section 7.7 of this Handbook;
- *customer* has a complex, higher risk structure – section 7.8 of *this Handbook*;
- *customer* is provided with private banking services – section 7.9 of this Handbook;
- *customer* is a personal asset holding vehicle – section 7.10 of this Handbook;
- *customer* is a company with nominee shareholders or issues bearer shares – section 7.11 of this Handbook;
- correspondent banking or similar relationships – section 7.12 of this Handbook.

3. It may be that *CDD* measures routinely applied under Article 13 of the *Money Laundering Order* already address some of the risk characteristics of these *customer*s (for instance identification of beneficial owner(s) and understanding the nature and purpose of the relationship) and significantly reduce the risk of *money laundering*, the *financing of terrorism* and *proliferation financing*. Therefore, any additional measures may be quite limited.

4. Nevertheless, the *enhanced CDD* measures required under Articles 15, 15A and 15B of the *Money Laundering Order* must be in addition to the measures to be taken in circumstances presenting a lower or standard risk, as set out in sections 4 and 6 of this Handbook and must address the particular risk presented. This section provides some (non-exhaustive) examples for each category of *customer*.

5. When applying *enhanced CDD* measures, a *supervised person* should not use a 'one size fits all' approach, e.g., applying the same package of measures regardless of the circumstances. The measures utilised should be tailored and appropriate to the specific scenario. The *supervised person* should also be able to articulate why they have applied the measures they have chosen, how they address the specific risks posed by the *customer* and how they are appropriate and commensurate with those risks.

6. A *customer* may be an individual (or group of individuals) or a legal person. Section 4.3 of this Handbook deals with the obligation to find out identity and obtain evidence for a *customer* who is an individual (or group of individuals), section 4.4 of this Handbook deals with the obligation to find out identity and obtain evidence for a *customer* (an individual or legal person) who is acting for a legal arrangement, and section 4.5 of this Handbook deals with the obligation to find out identity and obtain evidence for a *customer* who is a legal person.

7. References to a *customer* include, where appropriate, a prospective *customer* (an applicant for business) with whom a *business relationship* is to be established, or a *one-off transaction* carried out.

7.2 Requirement to apply *enhanced CDD measures*

Statutory requirements (paraphrased wording)

8. *Article 11(3)(c) of the Money Laundering Order requires a relevant person to maintain appropriate and consistent policies and procedures to determine whether:*

i. a customer;

ii. a beneficial owner or controller of a customer;

iii. a third party for whom a customer is acting;

iv. a beneficial owner or controller of a third party described in (iii);

v. a person acting, or purporting to act, on behalf of a customer; or

vi. a beneficiary under a life insurance policy,

vii. is a PEP.

9. *Article 11(3)(d) of the Money Laundering Order requires a relevant person to maintain appropriate and consistent policies and procedures to determine whether a business relationship or one-off transaction is with a person connected with a country or territory that does not apply, or insufficiently applies, the FATF Recommendations.*

10. *Article 15(1) of the Money Laundering Order requires a relevant person to apply enhanced CDD measures on a risk-sensitive basis in the following circumstances:*

a) if a customer has, or proposes to have, a business relationship or proposes to carry out a one-off transaction with the relevant person and the relevant person is not resident in the customer's country of residence or in the same country as the country from which, or from within which, the customer is carrying on business;

b) if a customer has not been physically present for identification purposes;

c) if the relevant person has or proposes to have a business relationship or proposes to carry out a one-off transaction with a customer having a relevant connection with a country or territory (an "enhanced risk state") in relation to which the FATF has called for the application of enhanced customer due diligence measures;

d) if the customer of the relevant person is a company with nominee shareholders or that issues shares in bearer form;

da) if the customer of the relevant person is a limited liability company with nominee limited liability company interest holders;

e) if the customer of the relevant person is:

i) *a legal person established by an individual for the purpose of holding assets for investment purposes; or*

ii) *a person acting on behalf of a legal arrangement established for an individual for the purpose of holding assets for investment.*

f) *if the relevant person provides or proposes to provide a customer with private banking services;*

g) *any situation which by its nature can present a higher risk of money laundering.*

7.3 Higher risk *customer*

Overview

11. Section 3.3 of this Handbook explains the risk-based approach to identification measures. It explains that a supervised person must, based on information collected, assess the risk that a business relationship or one-off transaction will involve money laundering, the financing of terrorism, or the financing of proliferation.

12. *Enhanced CDD measures* must be applied where a *supervised person's* assessment is that there is a higher risk of *money laundering,* the *financing of terrorism,* or the *financing of proliferation* (i.e., a situation which by its nature can present a higher risk of *money laundering,* the *financing of terrorism,* or the *financing of proliferation*).

13. There are several reasons why a *business relationship* or *one-off transaction* might be assessed as presenting a higher risk. For this reason, there are several possible measures listed in this section to address that risk.

Guidance notes

14. A *supervised person* may demonstrate that it has applied enhanced *identification measures* to an individual who is a higher risk *customer* under Article 15 of the *Money Laundering Order* where it obtains evidence that verifies a:

› former name (if applicable); or

› passport or national identity card number.

15. A *supervised person* may demonstrate that it has applied enhanced *identification measures* to a higher risk *customer* under Article 15(1)(g) of the *Money Laundering Order* where it takes reasonable measures to find out the ***source of funds*** and ***source of wealth*** at the time that a *business relationship* is established or *one-off transaction* carried out which are commensurate with risk and include one or more of the following:

› commissioning an independent and reliable report from a specialist security agency about the *source of funds* involved and/or *customer's source of wealth*;

› where a *supervised person* is part of a group, obtaining reliable information from the group's internal security department or business intelligence unit (or equivalent) about the *source of funds* involved and/or *customer's source of wealth*;

› where a *supervised person* is part of a group, obtaining reliable information from a part of the group which has an office in the country or territory with which the *customer* has a connection about the *source of funds* involved and/or *customer's source of wealth*;

› obtaining reliable information directly from the *customer* concerned, for instance during (or subsequent to) a face-to-face meeting inside or outside Jersey, or via a telephone "welcome call" on a home or business number which has been verified or by obtaining certified copies of corroborating documentation such as contracts of sale, property deeds, salary slips, etc.

- obtaining reliable information from an external party (for instance a Lawyer, *Accountant* or *tax adviser*) which has an office in the country or territory with which the *customer* has the connection about the *source of funds* involved and/or *customer's source of wealth*;
- A *supervised person* who obtains information from an external party should not accept such information on face value but should assess whether it is reasonable to use this information, e.g. is it complete and accurate to the standards required under Jersey law; how far removed from the *Beneficial owner and/or controller* are they; does this create any additional *AML/CFT/CPF* risks that should be factored into the *CRA*?
- obtaining reliable information from a person eligible to be an *obliged person* (for instance a Lawyer, *Accountant* or *tax advisor*) about the *source of funds* involved and/or *customer's source of wealth*;
- where information is publicly available or available through subscription databases, obtaining reliable information from a public or private source about the *source of funds* involved and/or *customer's source of wealth*;
- obtaining reliable information through financial statements that have been prepared in accordance with generally accepted accounting principles and audited in accordance with generally accepted auditing standards;
- establishing how the *source of funds* and *source of wealth* relate to the property which is or will be the subject of the *business relationship* or *one-off transaction.* For example, the *customer*'s funds, generated by their employment at an investment firm, were used to purchase a house which will be settled into a trust.

16. Where a connection is established during the course of an existing relationship, a *supervised person* may also demonstrate that it has taken reasonable measures to find out the *source of funds* and/or *source of wealth* where it reviews the relationship information that it already holds and concludes that it is reliable.

17. Where the measures set out in paragraphs 14 to 16 above are not sufficient to mitigate the risk associated with the *customer*, a *supervised person* may demonstrate that it has applied enhanced *identification measures* where it does one or more of the following in a way that is commensurate with risk:

- in a case where a document that has been used to obtain evidence of identity for a higher risk *customer*, e.g., a passport, subsequently expires, a *supervised person* may demonstrate that documents, data or information obtained under *identification measures* are kept up-to-date and relevant where a copy of the document that replaces that originally used to obtain evidence of identity is requested and obtained;
- in a case where a *business relationship* is to be established making use of a suitable certifier, it obtains confirmation that a photograph contained in the document certified bears a true likeness to the individual requesting certification (or words to that effect).

7.4 *Customer not physically present for identification measures*

Overview

18. Frequently, *business relationships* will be established, and *one-off transactions* carried out where there is no face-to-face contact with the *customer* to be identified or its *Beneficial owners and/or controllers*, for example:

- relationships established with individuals by mail, telephone or via the internet where external data sources are used to obtain evidence of identity;
- where identity is found out on persons who fall within Article 3(7) of the *Money Laundering Order* through a trustee or general partner, or on *Beneficial owners and/or controllers* of a legal person through that legal person.

19. There may also be circumstances where there is face-to-face contact with a *customer*, but where documentary evidence is to be provided at a time when the *customer* is not present.

20. Such circumstances may increase the risk of *money laundering,* the *financing of terrorism,* or the *financing of proliferation* as it may be easier for criminals to conceal their true identity when there is no face-to-face contact with the *supervised person*. They may also increase the risk of impersonation or identity fraud being used to establish a *business relationship* or conduct a *one-off transaction* for illegitimate purposes.

21. For the avoidance of doubt, this section does not apply to a person whose identity has been verified through a suitable certifier, (e.g., **where the certifier has met the person at the time the documents are certified**).

Statutory requirements (paraphrased wording)

22. *Under Article 15(1)(b) of the Money Laundering Order, if a customer has not been physically present for identification purposes, a relevant person must apply enhanced CDD measures on a risk-sensitive basis.*

AML/CFT/CPF Codes of Practice

[COP67] A *supervised person* must apply enhanced CDD measures on a risk-sensitive basis where a person who falls within Article 3(7) of the *Money Laundering Order*, or who is the Beneficial owner and/or controller of a *customer* or is a person who must otherwise be identified under Article 3 of the *Money Laundering Order*, is not physically present for identification purposes.

Guidance notes

23. A *supervised person* may demonstrate that it has applied enhanced *identification measures*:

- under Article 15 of the *Money Laundering Order*; and
- under the *AML/CFT/CPF Codes of Practice* set in COP67 above:

  Where it finds out further information on a person (in this example, “Person A”), obtains an additional form of evidence of identity for Person A, or carries out some other additional measure in respect of Person A.

24. Additional forms of evidence of identity may include use of a further source listed in section 4 of *this Handbook* (including independent data sources).

25. Other additional measures may include:

- where a *supervised person* is part of a group, confirmation from another part of that group that Person A has been met face-to-face;
- confirmation from a *supervised person* that carries on a *regulated business* or a person who carries on an *equivalent business* that Person A has been met face-to-face;
- confirmation from a *supervised person* that carries on *Trust Company Business* or a person who carries on an *equivalent business* that Person A is known to the *TCSP*, and the *TCSP* is satisfied that the particular individual is the person whose identity is to be found out;
- a combination of other checks that adequately take into account the *supervised person's* risk assessment for Person A, including:
  - requiring the first payment for the product or service to be drawn on an account in the *customer's* name at a bank that is a *regulated person* or carries on *equivalent business* (refer to section 1.8 of *this Handbook*);
  - telephone contact with the *customer* prior to establishing a relationship on a home or business number which has been verified, or a "welcome call" to the *customer* before transactions are permitted, using the call to verify additional components of identity found out;
  - internet sign-on following verification measures where the *customer* uses security codes, tokens, and/or other passwords which have been set up during account opening and provided by mail (or secure delivery) to the named individual at an independently verified address;
  - specific card or account activation measures.

7.5 *Customer* with *relevant connection* to an *enhanced risk state*

Overview

26. The *FATF* has identified a number of countries and territories which have failed to address their own *money laundering*, the *financing of terrorism, or proliferation financing* risks, and/or have in place insufficient *AML/CFT/CPF* regimes, in relation to which it has called for the application of countermeasures. These countries or territories are referred to in the *Money Laundering Order* as *enhanced risk states*. A person with a *relevant connection* to these countries or territories presents a higher risk of being involved in *money laundering*, the *financing of terrorism,* or the *financing of proliferation*, and doing business with such a person also poses an increased risk.

27. For the purpose of applying Article 15(1)(c) of the *Money Laundering Order*, *enhanced risk states* are those listed in **Appendix D1** of *this Handbook*.

7.5.1 Application of enhanced *CDD* measures to a *customer* with a relevant connection to an enhanced risk state

Statutory requirements (paraphrased wording)

28. *Under Article 15(1)(c) of the Money Laundering Order, if the relevant person has or proposes to have a business relationship or proposes to carry out a one-off transaction with a customer having a relevant connection with a country or territory (an "enhanced risk state") in relation to which the FATF has called for the application of enhanced customer due diligence measures, a relevant person must apply enhanced CDD measures on a risk-sensitive basis.*

29. *Under Article 15(2)(a) of the Money Laundering Order, for the purpose of the Article 15(1)(c), a "customer" includes any of the following:*

- *a) a beneficial owner or controller of the customer;*
- *b) a third party for whom the customer is acting;*
- *c) a Beneficial owner or controller of a third party described above;*
- *d) a person acting, or purporting to act, on behalf of the customer.*

30. *Under Article 15(2)(b) of the Money Laundering Order a person has a relevant connection with an enhanced risk state if the person is:*

- *a) the government or a public authority of that state;*
- *b) in relation to that state, a foreign PEP (within the meaning of Article 15A);*
- *c) a person resident in that state;*
- *d) a person having an address for business in that state;*
- *e) A customer, where the source of the customer's funds is or derives from assets held in that state by the customer or by any person on behalf of the customer or income arising in that state.*

AML/CFT/CPF Codes of Practice

[COP68] The enhanced *CDD* measures applied to a *customer* with a relevant connection to an enhanced risk state must include:

- requiring any new *business relationship* (and continuation thereof) or *one-off transaction* to be approved by senior management;
- where there is a *relevant connection* because a *customer's source of funds* is, or derives, from:
  - i) assets held in the state by the *customer* or by any person on behalf of the *customer;* or
  - ii) income arising in the State, taking reasonable measures to find out the *customer's source of wealth*.

Guidance notes

31. A *supervised person* may demonstrate that it has taken reasonable measures to find out the *source of wealth* at the time that a *business relationship* is established, or *one-off transaction* carried out, where the measures taken are commensurate with risk and include one or more of the measures listed in paragraph 15 above.

32. Where a *relevant connection* is established during an existing relationship, a *supervised person* may also demonstrate that it has taken reasonable measures to find out the *source of wealth* where it reviews the relationship information that it already holds and concludes that it is reliable.

33. A *supervised person* may demonstrate that it has otherwise applied *enhanced CDD measures* where it does all the following:

- in a case where a document that has been used to obtain evidence of identity for a higher risk *customer*, e.g., a passport, subsequently expires, a *supervised person* may demonstrate that documents, data or information obtained under *identification measures* are kept up-to-date and relevant where a copy of the document that replaces that originally used to obtain evidence of identity is requested and obtained;
- in a case where a relationship is to be established making use of a suitable certifier, it obtains confirmation that a photograph contained in the document certified bears a true likeness to the individual requesting certification (or words to that effect);
- reviews the *business relationship* on at least an annual basis, including all documents, data and information obtained under *identification measures* in order to ensure that they are kept up-to-date and relevant;
- where monitoring thresholds are used, sets lower thresholds for transactions connected with the *business relationship*.

7.6 *Customer* who is a *Politically Exposed Person* (*PEP*)

Overview

34. Corruption by *PEPs* will inevitably involve serious crime, such as theft or fraud, and is of global concern. The proceeds of such corruption are often transferred to other countries and territories and concealed through private companies, trusts or foundations, frequently under the names of relatives or close associates of the perpetrator.

35. By their very nature, *money laundering* investigations involving the proceeds of corruption generally gain significant publicity and are therefore very damaging to the reputation of both the businesses and countries/territories concerned. This is in addition to the possibility of criminal charges.

36. Indications that a *customer* may relate to corruption include excessive revenue from “commissions” or “consultancy fees” or involvement in contracts at inflated prices, where unexplained “commissions” or other charges are paid to external parties.

37. The risk of handling the proceeds of corruption or becoming engaged in an arrangement that is designed to facilitate corruption, is greatly increased where the arrangement involves a *PEP*. Where the *PEP* also has connections to countries or business sectors where corruption is widespread, the risk is further increased.

38. The nature of *enhanced CDD measures* applied will be commensurate with the risk that is identified and nature of the *PEP* connection. In particular, the measures to be applied by a *supervised person* to a *PEP*:

- who is *the Minister* of Finance in a country that is prone to corruption may be very different to the measures to be applied to a senior politician with a limited portfolio in a country or territory that is not prone to corruption;
- as another example, the measures to be applied to a company that is a *listed entity*, the securities of which are traded on a recognised market, and which has an investor who is a

PEP with a 1% holding in the scheme, may be very different to a private company established exclusively to hold investments for a *PEP*.

39. As a result, there is no "one-size fits all" approach to applying *enhanced CDD measures* for *PEPs*. There are mandatory enhanced *CDD* measures that must be applied on a risk-sensitive basis by *supervised persons* for *PEPs* to whom Article 15A applies. Such measures are set out in sub-section 15A(2), which include:

- approval of a new or continuation of a relationship or a new one-off transaction by senior management
- measures to establish source of wealth of the PEP and source of funds involved in the business relationship or one-off transaction.

40. Whilst *PEP* status does not in itself incriminate individuals or entities, it will mean that the *customer* may be subject to *enhanced CDD measures*. The nature and scope of a *supervised person's* activities will generally determine whether the existence of *PEPs* in its *customer* base is a practical issue for the *supervised person*.

7.6.1 Determining whether a *customer* is a *PEP*

Statutory requirements (paraphrased wording)

41. *Article 15A(3) of the Money Laundering Order provides the following definitions of PEP categories, which include an immediate family member or a close associate of the person:*

"domestic PEP" *means a person who is an individual who is or has been entrusted with a prominent public function in Jersey including but not limited to:*

- *heads of state, heads of government, senior politicians;*
- *senior government, judicial or military officials;*
- *senior executives of state-owned corporations;*
- *important political party officials.*

"foreign PEP" *means a person who is an individual who is or has been entrusted with a prominent public function in a country or territory outside Jersey including but not limited to:*

- *heads of state, heads of government, senior politicians;*
- *senior government, judicial or military officials;*
- *senior executives of state-owned corporations;*
- *important political party officials.*

"prominent person" *means a person who is an individual who is or has been entrusted with a prominent public function by an international organisation.*

"prominent public function" *in relation to an international organisation, means a member of the senior management, including a director, deputy director, board member or other equivalent function.*

"immediate family member" *includes any of the following:*

- *a spouse;*
- *a partner, that is someone considered by their national law as equivalent or broadly equivalent to a spouse;*

- *children and their spouses or partners (as defined above);*
- *parents;*
- *grandparents and grandchildren;*
- *siblings.*

"close associate" *of a person includes any person who is known to maintain a close business relationship with the person, including a person who is in a position to conduct substantial financial transactions on behalf of the person.*

42. *Under Article 15A(4) of the Money Laundering Order, for the purpose of deciding whether a person is a close associate of a person, a relevant person need only have regard to information which is in that person's possession or is publicly known.*

Guidance notes –senior executives of state-owned corporations

43. *Senior executives of state-owned corporations* are those individuals with executive decision-making authority. For domestic corporations only this would not normally include non-executive directors, where they do not have such authority.

44. State-owned corporations, as referred to above, may include 'arm's length' corporations whereby the state was involved in the set-up of the corporation but does not own or 100% own the corporation.

7.6.2 *Enhanced CDD measures* in relation to PEPs

Statutory requirements (paraphrased wording)

45. *Article 15A of the Money Laundering Order applies to a relevant person:*

- *who has or proposes to have a business relationship with, or proposes to carry out a one-off transaction with, a foreign PEP; or*
- *who has or proposes to have a high-risk business relationship, or proposes to carry out a high-risk one-off transaction with, a domestic PEP or prominent person; or*
- *if any of the following is a foreign PEP or, in the case of a high-risk business relationship or one-off transaction, a domestic PEP or prominent person:*

  i) a Beneficial owner or controller of the customer of the relevant person;

  ii) a third party for whom the customer of the relevant person is acting;

  iii) a Beneficial owner or controller of a third party described in clause (ii) above;

  iv) a person acting or purporting to act on behalf of the customer of the relevant person.

46. *A relevant person to whom Article 15A of the Money Laundering Order applies must apply enhanced CDD measures on a risk-sensitive basis including:*

- *unless the relevant person is a sole trader, measures requiring a new business relationship or continuation of a business relationship or a new one-off transaction to be approved by the senior management of the relevant person;*
- *measures to establish the source of the wealth of the PEP and source of the funds involved in the business relationship or one-off transaction;*

- *measures to conduct the enhanced ongoing monitoring of that relationship; and*
- *if the relevant business relationship relates to a life insurance policy, measures requiring the senior management to be informed before any payment is made under the policy or any right vested under the policy is exercised.*

47. *In Article 15A:*

"enhanced ongoing monitoring" *means ongoing monitoring that involves specific and adequate measures to compensate for the higher risk of money laundering.*

"high risk"*, in relation to a business relationship or one-off transaction, means any situation which by its nature can present a higher risk of money laundering.*

"source of the wealth" *means the source generating the total net worth of funds of the politically exposed person, whether those funds are used in the business relationship or one-off transaction.*

48. *Under Article 15A(2A) a domestic politically exposed person is relieved of such status 2 years after the person ceases to be entrusted with a prominent public function if the relevant person is satisfied that:*

i) following a risk assessment, the person does not present a higher risk of money laundering; and

ii) there is no reason to continue to treat the person as a politically exposed person.

49. *Under Article 15A(2B) a foreign politically exposed person is relieved of such status after 5 years of the person ceasing to be entrusted with a prominent public function if the relevant person is satisfied that:*

i) following a risk assessment, the person does not present a higher risk of money laundering; and

ii) there is no reason to continue to treat the person as a politically exposed person.

50. *Under Article 15A(2C)* a prominent person is relieved of politically exposed person status 5 years after the person ceases to be entrusted with a prominent public function by an international organisation if the relevant person is satisfied that:

i) following a risk assessment, the person does not present a higher risk of money laundering; and

ii) there is no reason to continue to treat the person as a politically exposed person.

51. Under Article 15A(2D), Articles 15A(2A) to Article 15A(2C) also apply to immediate family members or close associates of the politically exposed person.

52. Article 15A(3) defines a prominent public function in relation to an international organisation as being a member of the senior management, including a director, deputy director, board member or other equivalent function.

AML/CFT/CPF Codes of Practice

[COP69] Policies and procedures maintained in line with Article 11 of the *Money Laundering Order* must recognise that *customer*s may subsequently acquire PEP status.

[COP70] A domestic PEP can only be considered as no longer being a PEP, two years after they cease to be entrusted with a prominent public function if, following a risk assessment, the person does not present a higher risk of *money laundering* and there is no reason to continue to treat the person as a PEP.

[COP71] A foreign PEP can only be considered as no longer being a PEP five years after they cease to be entrusted with a prominent public function if, following a risk assessment, the person does not present a higher risk of *money laundering* and there is no reason to continue to treat the person as a PEP.

[COP72] A prominent person can only be considered as no longer being a PEP five years after they cease to be entrusted with a prominent public function if, following a risk assessment, the person does not present a higher risk of *money laundering* and there is no reason to continue to treat the person as a prominent person.

Guidance notes

53. The *customer* will often be a key source of this information that will be collated during the *CDD* process at onboarding and during ongoing monitoring. It is good practice to require the *customer* as part of their terms of engagement to be required to self-identify themselves as a PEP, close associate or immediate family member of a PEP. However, this is not the sole method for identifying close associates. In line with Article 15A(2) of the Money Laundering Order, a relevant person is only required to consider information that is already in their possession or is publicly known when making this determination.

54. Summary of Enhanced *CDD* measures dependent on key PEP characteristics:

Type of PEP (includes close associates and family members)	Foreign *PEP*	Domestic *PEP*	*Prominent person*
Application of Enhanced *CDD* measures	All	High risk business relationship or one-off transaction only	High risk business relationship or one-off transaction only
May be declassified after ceased to act for period specified and prescribed conditions met.	5 years	2 years	5 years

Guidance notes – Foreign *PEPs*

55. The requirements in section 15A apply to relationships and one-off transactions with all foreign *PEPs* (such term always including their immediate family and close associates) not just high-risk foreign *PEPs*. For the avoidance of doubt Foreign means a PEP in a country or territory outside Jersey, for example which will include the United Kingdom and Guernsey.

56. A *supervised person* required to adhere to Jersey AML/CFT/CFP requirements that may be part of a Group located outside of Jersey should ensure that the Jersey requirements are met. For example, UK PEPs are foreign PEP's for Jersey purposes and the starting point is not that they should automatically be treated as lower risk.

57. Where the existence of foreign *PEPs* is a practical issue, a *supervised person* may demonstrate that it has appropriate *policies and procedures* for determining whether a *customer* or prescribed person is a *PEP* where it does the following:

- assesses those countries and territories to which *customers* are connected, which pose the highest risk of corruption. See section 3.3.4.1 of *this Handbook*;
- finds out who the current and former holders of prominent public functions are within those *higher risk countries and territories* and determines, as far as is reasonably practicable, whether *customers* have any connections with such individuals (including through immediate family or close associates). In determining who the current and former holders of prominent public functions are, it may have regard to information already held by the *supervised person* and to external information sources such as the *UN*, the European Parliament, the *UK* Foreign, Commonwealth & Development Office, the Group of States against Corruption, and other external data sources (see section 3.3.4.2 of *this Handbook*); and
- exercises vigilance where *customers* are involved in business sectors that are vulnerable to corruption such as (but not limited to) oil or arms trades.

58. Where a *supervised person* runs the details of all its *customers* and prescribed persons through an external data source (e.g., a screening package) to determine whether any of them are *PEPs*, it should nevertheless also assess those countries and territories to which *customers* are connected, which pose the highest risk of corruption, and exercise particular vigilance where *customers* are involved in business sectors that are vulnerable to corruption.

59. Where the *customer* is a *PEP* by virtue of their position as a senior executive of a sovereign wealth fund, the *supervised person* should check if the body is a member of the *IFSWF.* The *IFSWF* promotes transparency, good governance, and sound investment practices. Whilst membership of the *IFSWF* alone cannot guarantee that a sovereign wealth fund or senior executive thereof will act with integrity, the information provided on the *IFSWF'*s website regarding the sovereign wealth fund may support other *CDD* measures undertaken.

60. In a case where a *PEP* is a director (or equivalent) of a *customer*, or person acting or purporting to act for a *customer*, and where no property of that *PEP* is handled in the particular *business relationship* or *one-off transaction*, a *supervised person* may demonstrate that it applies specific and adequate measures under Article 15A(2) of the *Money Laundering Order* where it considers the nature of the *PEP's* connection and reason why the *PEP* has such a connection.

61. Similarly, where a *PEP* is a trustee or a general partner that is a *customer* or is a beneficiary or object of a power of a trust, and where no property of that *PEP* is handled in the particular *business relationship* or *one-off transaction*, a *supervised person* may demonstrate that it applies specific and adequate measures under Article 15A(2) of the *Money Laundering Order* where it considers the nature of the *PEP's* connection and reason why the *PEP* has such a connection.

7.6.2.1 **Declassification of foreign *PEP*s and *prominent persons***

62. For the purposes of declassification, immediate family members, and close associates of *foreign PEPs*, and *prominent persons,* should be treated like PEPs.

63. A declassification assessment may occur once the relevant time period has passed. The timing of such an assessment, if at all, is at the discretion of the *supervised person.*

64. When a *supervised person* is considering the declassification of foreign *PEPS*, *and prominent persons*, *supervised persons* might consider the following:

- The level of inherent corruption risk in the country of political exposure;
- The position held and its susceptibility to corruption or misappropriation of state funds or assets;
- Length of time in office and the likelihood of return to office in the future;

- The level of transparency about the source of wealth and origin of funds, in particular funds generated while in office;
- Links to any industries that are high risk for corruption;
- The overall plausibility of the stated *customer* profile and net worth;
- The level of transparency and plausibility of transactions processed through the account;
- Whether there is relevant adverse information about the *customer* published in reputable sources; and
- How politically connected they remain once they have left office.

65. For further guidance on declassifying PEPs *supervised persons* can refer to the following:

- *The Wolfsberg Group Guidance; and*
- *The FATF Guidance on Recommendation 12 and 22.*

Guidance notes – Domestic *PEPs*

66. The requirements in section 15A apply to high-risk business relationships or high-risk one-off transactions with domestic *PEPs or prominent persons* (such terms always including their immediate family and close associates).

67. In determining whether someone is a domestic *PEP*, a *supervised person* should consider the criterion set out at Article 15A(3) of the *Money Laundering Order* – namely that a *PEP* is an individual who is or has been entrusted with a prominent public function, for example:

- heads of state, heads of government, senior politicians;
- senior government, judicial or military officials;
- senior executives of state-owned corporations;
- important political party officials.

68. In the context of Jersey, this will include (but is not limited to) the following positions:

- Lieutenant-Governor;
- Ministers (but not necessarily deputy Ministers);
- Chief Executive of the States of Jersey;
- Director-Generals of the States of Jersey;
- HM Attorney-General;
- HM Solicitor-General;
- Commissioners of the *JFSC*;
- Director General of the *JFSC*;
- Registrar of Companies;
- Information Commissioner;
- Comptroller and Auditor-General;
- Bailiff;
- Deputy Bailiff;
- Judicial Greffier;

- Comptroller of Taxes;
- HM Receiver General;
- Senior Executives of state-owned Body Corporates (or similar).

69. Note that this will also include immediate family members and close associates of individuals listed above. It is good practice to periodically check that your *PEP*-related definitions align with those in Article 15A of the *Money Laundering Order* and *this Handbook* guidance.

70. Middle ranking or junior officials are unlikely to be *PEPs* unless their political exposure is comparable to that of a similar position at national level.

7.6.2.2 Declassification of domestic *PEP*s

71. A declassification assessment may occur once the relevant time period has passed. The timing of such an assessment, if at all, is at the discretion of the *supervised person.*

72. When a *supervised person* is considering the declassification of domestic *PEP*s, *supervised persons* might consider the following:

- The level of inherent corruption risk in the country of political exposure;
- The position held and its susceptibility to corruption or misappropriation of state funds or assets;
- Length of time in office and the likelihood of return to office in the future;
- The level of transparency about the source of wealth and origin of funds, in particular funds generated while in office;
- Links to any industries that are high risk for corruption;
- The overall plausibility of the stated *customer* profile and net worth;
- The level of transparency and plausibility of transactions processed through the account;
- Whether there is relevant adverse information about the *customer* published in reputable sources; and
- How politically connected they remain once they have left office.

73. *Supervised persons* may apply *enhanced CDD measures* for a longer period if required after considering the factors above and deciding the *PEP* should not be declassified.

74. For further guidance on declassifying domestic PEPs *supervised persons* can refer to the following:

- *The Wolfsberg Group Guidance; and*
- *The FATF Guidance on Recommendation 12 and 22.*

7.6.2.3 Higher risk domestic *PEPs*

75. As set out in Article 15A(1)(b) of the *Money Laundering Order*, mandatory *enhanced CDD measures* are only required in relation to *business relationships* or *one-off transactions* with domestic *PEPs* which are assessed as higher risk. This is not the case for foreign *PEPs* where *enhanced CDD measures* are required for all risk ratings.

76. Individuals entrusted with a prominent public function in Jersey may be considered to pose a low risk, unless a *supervised person* considers that other specific risk factors indicate a higher risk. Particular consideration should be given to the following characteristics that might indicate a higher risk:

- responsibility for, or ability to influence, large public procurement exercises;
- responsibility for, or ability to influence, allocation of government licenses (or similar);
- personal wealth or lifestyle inconsistent with known legitimate sources of income or wealth*;*
- credible allegations of financial misconduct.

77. Similarly, immediate family or close associates of individuals entrusted with a prominent public function in Jersey may be considered to pose a low risk, unless a *supervised person* considers that other specific risk factors indicate a higher risk. Particular consideration should be given to the following characteristics that might indicate a higher risk:

- wealth or lifestyle inconsistent with known legitimate sources of income or wealth;
- credible allegations of financial misconduct;
- wealth derived from the granting of government *Licence*s (or similar);
- wealth derived from preferential access to the privatisation of former state assets.

7.7 Non-resident *customer*

Overview

78. *Customers* who are not resident in a country or territory, but who nevertheless seek to form a *business relationship* or conduct a *one-off transaction* with a *supervised person* in that country or territory will typically have legitimate reasons for doing so. Some *customers* will, however, pose a risk of *money laundering,* the *financing of terrorism,* or the *financing of proliferation* and may be attempting to move illicit funds away from their country or territory of residence or attempting to further conceal funds sourced from that country or territory.

Statutory requirements (paraphrased wording)

79. *Under Article 15(1)(a) of the Money Laundering Order, if a customer has, or proposes to have, a business relationship or proposes to carry out a one-off transaction with the relevant person and the relevant person is not resident in the customer's country of residence or in the same country as the country from which, or from within which, the customer is carrying on business, a relevant person must apply enhanced customer due diligence measures on a risk-sensitive basis.*

Guidance notes

80. A *supervised person* may demonstrate that it has applied *enhanced CDD measures* under Article 15(1)(a) of the *Money Laundering Order*, where it has applied additional measures that are commensurate with risk. Additional measures may include one or more of the following:

- determining the reasons why the *customer* is looking to establish a *business relationship* or carry out a *one-off transaction* other than in their home country or territory; and/or
- the use of external data sources to collect information on the *customer* and the country risk of the *customer's* home country or territory (see section 3.3.4.1 of *this Handbook*) to build a *customer* business and risk profile similar to that available for a resident *customer*.

7.8 Complex higher risk structures

AML/CFT codes of practice

[COP73] A supervised person must apply proportionate and relevant enhanced due diligence to a customer where the structure is complex, and the complexity contributes to the customer being assessed as high-risk.

7.8.1 CDD to EDD trigger and scope

Guidance notes

81. Where a customer or a linked arrangement relevant to beneficial ownership, control, or purpose is complex, that complexity alone does not trigger enhanced customer due diligence (EDD). If the rationale for the complexity remains unclear, insufficiently evidenced or where beneficial ownership and control information is incomplete and further enquiry is required, this may lead to the customer being identified as high-risk, triggering the requirement for EDD. Where transparency cannot be achieved after reasonable enquiries and application of proportionate EDD, *supervised persons* should consider declining or exiting the relationship and assess any suspicious activity reporting obligations. EDD centres on the customer and surrounding arrangements are considered only to the extent needed to establish beneficial ownership and/or control and purpose of the structure.

82. Enhanced CDD measures may include one or more of the following. This list is non-exhaustive.

a. <u>Establishing Legitimacy</u>

- Most supervised persons obtain rationale and structure charts as part of CDD measures. Enhancements may include obtaining supporting documentation (e.g. legal opinions, tax advice, professional advice, board/executive approvals, transaction papers, minutes) that evidence the purpose and legitimacy of the structure proportionate to the risk (this does not presume advice exists for the entire structure).
- Where a structure is complex and high-risk but standardised and ultimately transparent, supervised persons may document the rationale for proportionate EDD in their policies and confirm it applies to the customer, with any adjustments, instead of repeating the full EDD each time.

b. <u>Source of Wealth and Funds</u>

- Where the complexity of a structure requires enhanced CDD measures to verify beneficial owners source of funds and source of wealth proportionate to the risk. EDD may be achieved by obtaining independent documentation such as audited financials, bank statements, or asset sale agreements (see also section 7.3 paragraph 15)

  Controllers who do not contribute funds and have no economic interest would not normally require source of wealth/source of funds. It may be necessary to obtain targeted information only where controllers contribute funds, exercise material control creating financial crime risk, or where other red flags may be present.

c. <u>Understanding transactional flows (where flows drive the complexity)</u>

- Evidence an understanding of expected flows within the structure (e.g. funding, distributions, fees) and assess unusual routings that lack commercial purpose.

d. Independent Verification

› Where proportionate, use independent sources or external experts (e.g. due diligence reports, legal/accounting opinions, forensic reviews) to corroborate rationale, ownership/control, or fund flows.

e. Face to Face

› In high-risk cases consider meeting the ultimate beneficial owner in person or equivalent where feasible.

Where existing high-risk monitoring does not already address the risks relating to complexity the measures below may be applied in conjunction with other enhanced CDD measures.

f. Ongoing Monitoring

› Monitoring frequency should be adjusted where complexity materially increases risk beyond the *supervised person*'s baseline high-risk schedule.

› Set enhanced triggers for re-assessment.

g. Senior Management Approval

› Require sign-off from senior management before onboarding or continuing where the relationship is assessed as high-risk and complexity contributes to that rating, documenting residual risk and mitigations.

7.9 *Customer* provided with private banking services

Overview

83. Private banking is generally understood to be the provision of banking and investment services to high-net- worth *customers* in closely managed relationships. It often involves complex, bespoke arrangements and high value transactions across multiple countries and territories. Such *customers* may therefore present a higher risk of *money laundering,* the *financing of terrorism,* or the *financing of proliferation*.

84. A trustee who may from time to time facilitate such banking or investments services as part of carrying on *Trust Company Business* is not considered to be providing private banking services, where such facilitation is ancillary to the core business of acting as a trustee.

Statutory requirements (paraphrased wording)

85. *Under Article 15(1)(f) of the Money Laundering Order, if the relevant person provides or proposes to provide a customer with private banking services, a relevant person must apply enhanced CDD measures on a risk-sensitive basis.*

86. *Under Article 15(3), a service is a "private banking service" if the service is offered, or it is proposed to offer the service, only to persons identified by the service provider as being eligible for the service, having regard to the person's net worth, and the service:*

a) involves a high value investment;

b) is a non-standard banking or investment service tailored to the person's needs, or uses corporate or trust investment structures, tailored to the person's needs; or

c) offers opportunities for investment in more than one jurisdiction.

Guidance notes

87. A *supervised person* may demonstrate that it has applied *enhanced CDD measures* under Article 15(1)(f) of the *Money Laundering Order* in respect of a private banking relationship, where it has applied additional measures that are commensurate with risk. Additional measures may include:

- taking reasonable measures to find out the *source of funds* and *source of wealth;*
- reviewing the *business relationship* on at least an annual basis, including all documents, data and information obtained under *identification measures* in order to ensure that they are kept up-to-date and relevant;
- where monitoring thresholds are used, setting lower thresholds for transactions connected with the *business relationship*.

7.10 *Customer* that is a personal asset holding vehicle

Overview

88. Personal asset holding vehicles are legal persons or legal arrangements established by individuals for the specific purpose of holding assets for investment. The use of such persons or arrangements may make identification of ultimate beneficial owners more difficult since layering of ownership may conceal the true source or controller of the investment.

89. Article 15(1)(e) of the *Money Laundering Order* is intended to apply in two specific scenarios:

- where the personal asset holding vehicle is the *customer*; or
- where the personal asset holding vehicle is the third party for whom a trustee or general partner (the *customer*) is acting.

Guidance notes

90. A *supervised person* may demonstrate that it has applied *enhanced CDD measures* under Article 15(1)(e) of the *Money Laundering Order*, where it has applied additional measures that are commensurate with risk. Additional measures may include:

- understanding the structure of the vehicle, determining the purpose and rationale for making use of such a vehicle, and being satisfied that the *customer's* use of such an investment vehicle has a genuine and legitimate purpose;
- taking reasonable measures to find out and document the *source of funds* and *source of wealth*.

7.11 Customer that is a company with nominee shareholders or issues bearer shares

Overview

91. Companies with nominee shareholders or bearer shares (or the ability to issue bearer shares in the future) may present a higher risk because such arrangements make it possible to hide the identity of the *beneficial owner(s)* and/or changes in beneficial ownership by separating legal and beneficial ownership, or because there is no trail of ownership, which introduces a degree of anonymity.

92. Nevertheless, nominee shareholders are often used for good and legitimate reasons, e.g., to ease administration and reduce client costs by enabling a nominee to take necessary corporate actions, such as the passing of resolutions, in the day-to-day administration of a corporate structure.

93. Where one or more of the following circumstances apply, the *customer* **should not** be considered to be a *customer* that issues bearer for the purpose of Article 15(1) of the *Money Laundering Order*:

- › the bearer shares are issued by a company in a country or territory that has fully enacted appropriate legislation to require bearer shares to be registered in a public registry and the bearer shares are so registered; or
- › the bearer shares are traded on an approved stock exchange; or
- › all issued bearer shares are held in the custody of the *supervised person*, the *customer* or trusted external party along with an undertaking from that trusted external party or *customer* to inform the *supervised person* of any transfer or change in ownership.

Statutory requirements (paraphrased wording)

94. *Under Article 15(1)(d) of the Money Laundering Order, if a customer of a relevant person is a company with nominee shareholders or that issues shares in bearer form, a relevant person must apply enhanced CDD measures on a risk-sensitive basis*.

Guidance notes

95. A *supervised person* may demonstrate that it has applied *enhanced CDD measures* under Article 15(1)(d) of the *Money Laundering Order*, where it has applied additional measures that are commensurate with risk.

96. In the case of *customers* who are companies with nominee shareholders, additional measures may include:

- › determining and being satisfied with the reasons why the *customer* is making use of nominees;
- › using external data sources to collect information on the fitness and propriety of the nominee (such as its regulated status and reputation) and the particular country risk.

97. In the case of *customers* who are companies with bearer shares (or the ability to issue bearer shares in the future), additional measures may include:

- › determining and being satisfied with the reasons why the *customer* has issued bearer shares or retains the ability to do so;
- › ensuring that any new or continued *business relationship* or any *one-off transaction* is approved by the *senior management* of the *supervised person*;
- › reviewing the *business relationship* on at least an annual basis, including all documents, data and information obtained under *identification measures* to ensure that they are kept up to date and relevant.

7.12 Correspondent banking and similar relationships

Overview

98. **Correspondent Banking** is defined as the provision of *Banking Services* by a *Jersey financial institution* or *VASP* (i.e. the **correspondent**) to a *foreign financial institution* or *VASP* that itself provides *Banking Services* to its *customers* (i.e. the **respondent**, but only where the *respondent* is not in Jersey).

99. **Banking Services** include the following:

- providing a current or other liability account;
- cash management;
- international funds transfers;
- cheque clearing;
- providing *customer*s of the respondent with direct access to accounts with the correspondent (and vice versa); and
- providing foreign exchange services.

100. In accordance with the *FATF* standard, *Supervised Persons* that are *financial institutions* and *VASPs* must also apply enhanced measures in relation to *similar relationships,* being those where financial services other than *Banking Services* are provided by the *supervised person* (the correspondent) to an overseas *financial institution or VASP* (the respondent) for the benefit of *customer*s of the respondent, including for example, those established for securities transactions. The degree of *AML/CFT* risk in such relationships is different, generally lower, than it is with relationships which provide for *Banking Services*; they are more similar to normal *customer* relationships.

101. As a result, in both cases (*correspondent banking and similar relationships*), the correspondent makes its services available to the *customer*s of the *respondent*. In doing so, the correspondent potentially exposes itself to additional risk. This section sets out the additional *CDD measures* required by the *Money Laundering Order* to appropriately manage the risk presented by such relationships and provides guidance.

102. *Jersey financial institutions and VASPs* are prohibited by the *Money Laundering Order* from entering into correspondent *banking relationships* with shell banks and must take steps to ensure they do not provide *correspondent banking services* to banks that *permit shell banks* to have accounts.

Statutory requirements (paraphrased wording)

103. *Article 15B of the Money Laundering Order applies to a Jersey VASP which has or proposes to have a correspondent banking or similar relationship with a foreign financial institution or foreign VASP. Article 15B of the Money Laundering Order applies to a Jersey financial institution or VASP who has or proposes to have a correspondent banking or similar relationship with a financial institution or VASP whose address for that purpose is outside Jersey.*

104. *Under Article 15B(2) of the Money Laundering Order a Jersey financial institution or VASP must apply enhanced customer due diligence measures on a risk-sensitive basis including:*

- *gathering sufficient information about the institution to understand fully the nature of its business;*
- *determining the reputation of the institution and the quality of its supervision, including whether it has been subject to any money laundering investigation or regulatory action;*

- *assessing the institution's systems and controls to combat money laundering in order to determine whether they are consistent with the requirements of the FATF recommendations and their effectiveness;*
- *requiring any new relationship to be approved by the senior management of the relevant person;*
- *ensuring that both the relevant person and the institution clearly understand their respective responsibilities to prevent and detect money laundering and recording those responsibilities;*
- *being satisfied that, in respect of customers of the institution who have services provided directly by the relevant person, that the institution has applied customer due diligence measures at least equivalent to those set out in this Order and is able to provide a copy, at the request of the relevant person, of the evidence, documents, data and information obtained when applying such measures.*

105. *Article 23A(1) of the Money Laundering Order provides that a Jersey financial institution or VASP must not enter into a correspondent banking relationship, or continue an existing correspondent banking relationship, with a respondent that is a shell bank.*

106. *Article 23A(2) of the Money Laundering Order provides that a Jersey financial institution or VASP must take appropriate measures to ensure that it does not enter into a correspondent banking relationship, or continue an existing correspondent banking relationship, with a financial institution or VASP that is known to permit its accounts to be used by a shell bank.*

107. *Article 23A(4)(b) defines "shell bank" as a bank incorporated in a jurisdiction in which it has no physical presence involving meaningful decision-making and management, and which is not subject to supervision by the JFSC or by an overseas regulatory authority by reason of that bank's connection with any other institution or person.*

- *assessing the systems and controls of the foreign financial institution or foreign VASP to combat money laundering in order to determine whether they are consistent with the requirements of the FATF Recommendations and their effectiveness;*
- *requiring any new relationship to be approved by the senior management of the Jersey financial institution or Jersey VASP.*

Guidance notes

108. This part of the *Money Laundering Order* and this guidance applies to *supervised persons* that are *financial institutions or VASPs* that have *correspondent banking* or *similar relationships* with an overseas *financial institution or VASP*.

109. The *respondent's* address for this purpose should be considered to be overseas unless the transaction is with the *Jersey office* of a business.

110. A *correspondent* may demonstrate that it has gathered sufficient information about the respondent where it obtains information concerning the following:

- the geographic location of its *customer* base;
- the general nature of its *customer* base;
- the nature of the services which the Institution provides to its *customers*;
- whether relationships are conducted by the Institution on a non-face to face basis;

› the extent to which the institution relies on third parties to identify and hold evidence of identity or to conduct other *CDD measures* on *customer*s.

111. A *supervised person* may determine the respondents' reputation by assessing its stature from publicly available information from credible sources on the reputation of the *respondent* and the quality of the supervision to which it is subject.

112. A *correspondent* may determine that a *respondent's* systems and controls are consistent with the requirements of the *FATF Recommendations* where the *respondent* carries on equivalent business (see Section 1.8 of *this Handbook*).

113. Where *customer*s of the *respondent* have direct access to the services of the *correspondent*, a *correspondent* may satisfy itself as to the adequacy of the respondent's *CDD measures*, and its ability to provide relevant *CDD* information and documents on request where either:

a) It obtains a written assurance from the *respondent* to this effect; or

b) The *correspondent bank* may also satisfy itself as to the adequacy of the *CDD measures* of the r*espondent* and its ability to produce information and documentation on request by periodically requesting relevant *CDD* information and documents from the institution.

114. Where the *correspondent* provides *correspondent banking*, the *correspondent* should also consider the following guidance:

a) Correspondent Banking Services (FATF);

b) Correspondent Banking Principles (Wolfsberg Group);

c) *Money laundering* – UK Joint Money Laundering Steering Group's Guidance (JMLSG), Part II, Chapter 16 - the guidance relating to "Correspondent Banking Relationships".

115. For *similar relationships*, it should also consider the following guidance:

a) *Money laundering* – UK Joint Money Laundering Steering Group's Guidance (JMLSG),Part II, Chapter 16 - the guidance relating to "Correspondent Trading Relationships".

116. Regarding the definition of a *shell bank,* "physical presence" means meaningful mind and management located within a country. The existence simply of a local agent or low-level staff does not constitute physical presence.

7.13 *Enhanced CDD measures* – transitional arrangements

Overview

117. Where amendments to the *Money Laundering Order* introduce new *CDD* requirements applicable to *business relationships* and *one-off transactions*, these requirements do not apply retrospectively, and no remediation project is required.

118. However, Article 13(1)(c)(ii) of the *Money Laundering Order* requires a *supervised person* to apply *identification measures* where the *supervised person* has doubts about the veracity or adequacy of documents, data or information previously obtained. In the context of this section, this would include where documents, data or information previously obtained for a *business relationship* do not satisfy additional new *CDD* requirements, such as those set out in the *Money Laundering (Amendment No.10) (Jersey) Order 2019*.

119. This means that where, during the course of its regular review of a *business relationship* (pursuant to Article 3(3)(b) of the *Money Laundering Order* and discussed at section 6 of *this Handbook*) a *supervised person* becomes aware that documents, data or information previously obtained do not satisfy the additional *CDD* requirements set out in the *Money Laundering (Amendment No.10) (Jersey) Order 2019* (or any other subsequent amendments), the *supervised person* will need to apply *CDD* measures to that *customer* at that time, in line with the requirement in Article 13(1)(c)(ii) of the *Money Laundering Order.*

8 EXEMPTIONS FROM *CDD* REQUIREMENTS

Overview

1. Part 3A of the *Money Laundering Order* provides for exemptions from *CDD* requirements that apply in some strictly limited circumstances, as set out in Articles 17B - D and 18 of the *Money Laundering Order*.

MLO Article	Exemption	*Handbook* section
17B	Exemptions from applying third party identification requirements in relation to relevant *customer*s acting in certain regulated, investment or fund services business.	Section 8.2
17C & 17D	Exemptions from applying third party identification requirements in relation to certain relevant *customer*s involved in unregulated or non-public funds, Trust Company Business or the legal profession.	Section 8.3
18	Further exemptions from applying identification requirements to *customers*.	Section 8.4

2. **All exemptions under Articles 17A-D and Article 18 still require a level of *CDD*** to be performed. Requirements are outlined in the above referenced section of *this handbook*.

8.1 Limits to applying exemptions

3. Article 17A of the *Money Laundering Order* provides pre-requisite circumstances in which exemptions under Part 3A do not apply. See the table below:

Circumstances in which exemptions under Part 3A of the *Money Laundering Order* do not apply (Article 17A *of the Money Laundering Order)*	
Exemptions under Articles 17 B-D of the *Money Laundering Order*	**Exemptions under Article 18 of the *Money Laundering Order***
› the *supervised person* **suspects *money laundering***	› the *supervised person* **suspects *money laundering***
› the *supervised person* **considers that there is a higher risk of *money laundering***, including the risk of *money laundering* if fail to apply appropriate *identification measures* or keep records	› the *supervised person* **considers that there is a higher risk of *money laundering***
› the *customer* is resident in a **country that is not compliant with the *FATF Recommendations*** › the *customer* is a person in respect of whom Article 15(1)(c) of the *Money Laundering Order* applies [specified persons having a *relevant connection* to **country/territory in relation to which *FATF* has called for *enhanced CDD* measures**].	› the *customer* is resident in a **country that is not compliant with the *FATF Recommendations*** › the *customer* is a person in respect of whom Article 15(1)(c) of the *Money Laundering Order* applies [specified persons having a *relevant connection* to **country/territory in relation to which *FATF* has called for *enhanced CDD* measures]**.

4. It is important to note that these specific scenario-based exemptions should only be applied when all conditions or criteria are met. For the exemption that requires a risk assessment, it should only be used where the risk is assessed as low. If there is higher risk of money laundering the exemptions should not apply.

Guidance notes

5. Definitions for various terms used within Part 3A of the *Money Laundering Order* and this section are set out below (save that *relevant person* is replaced with *supervised person*):

› ***Relevant customer*** means a *customer* of a *supervised person* that the *supervised person* knows or reasonably believes is:

  - a *supervised person* in respect of whose *financial services business* the *JFSC* discharges supervisory functions, or a person carrying on *equivalent business;* or
  - a person wholly owned by a *supervised person* described in the above point (the "parent"), but only if:
    - the person is incorporated or registered in the same jurisdiction as the parent;
    - the person has no *customer*s who are not *customer*s of the parent;
    - the person's activity is ancillary to the business in respect of which the *JFSC* discharges supervisory functions, or to *equivalent business* carried on by the parent; and
    - in relation to that activity, the person maintains the same *policies and procedures* as the parent.

› ***third party identification requirements*** mean the requirements of Articles 13 or 15, 15A, 15B of the *Money Laundering Order to* apply the *identification measures* specified in Article 3(2)(b) of the *Money Laundering Order.*

› **non-public fund** means a scheme falling within the definition of "collective investment fund" in Article 3 of the *CIF(J) Law*, except that the offer of units in the scheme or arrangement is not an offer to the public within the meaning of that Article.

6. Exemptions from *identification measures* may only be applied in appropriate circumstances. Where specified, this will require an assessment of the risk of applying the exemption, in addition to a *CRA*. Exemption from applying third party identification requirements in relation to relevant customers acting in certain regulated, investment or fund services business (Article 17B)

8.1.1 This is a blank paragraph

Statutory requirements (paraphrased wording)

7. *Under Article 17B(1) of the Money Laundering Order, a relevant person is exempt from applying third party identification requirements in relation to a third party for which a relevant customer is acting where the relevant customer is acting in the course of a business:*

› *that falls within paragraphs (a), (b) or (d) in the definition of "regulated business" in Article 1, or equivalent business; or*

› *that is an investment business or fund services business registered under the FS(J) Law, or equivalent business.*

8. *Under Article 17B(2) of the Money Laundering Order, a relevant person must record the reasons for applying the exemption, having regard to the risk of money laundering inherent in the relevant customer's business and the higher risk of money laundering associated with that type of business should the relevant customer fail to:*

a) *apply the identification measures specified in Article 3(2)(b) of the Money Laundering Order, or if the relevant customer is not in Jersey, similar identification measures required to be applied to satisfy the requirements in Recommendation 10 of the FATF Recommendations; or*

b) *keep records, or keep them for the period required to be kept.*

AML/CFT/CPF Codes of Practice

[COP74] A *supervised person* must be able to demonstrate that the exemption conditions required by the *Money Laundering Order* and summarised in the *statutory requirements* above are being met.

Guidance notes

8.1.2 Assessment of risk

Overview

9. The risk factors that are set out in this section will also be relevant to a *CRA* that is conducted under section 3.3.4.1 of *this Handbook* in the cases highlighted at sections 4.3 and 4.5 of *this Handbook*.

Statutory requirements (paraphrased wording)

10. *Immediately before applying the exemptions set out in Article 17B(1), Article 17B(2) of the Money Laundering Order requires a relevant person to conduct an assessment as to whether it is appropriate to do so, having regard to the relevant customer's business and the higher risk of money laundering should the relevant customer fail to:*

› *apply the necessary identification measures to its customer(s); or*

› *keep records, or keep them for the period required to be kept.*

11. *Article 17B(2) of the Money Laundering Order requires a relevant person to prepare a written record of the reason why it is appropriate to apply CDD exemptions.*

Guidance notes

12. Immediately before applying the exemptions set out in Article 17B(1) of the *Money Laundering Order*, a *supervised person* may demonstrate that it has had regard to a *relevant customer*'s business where it considers the following factors:

› the general risk appetite of the *relevant customer*;

› the geographic location of the *relevant customer*'s client base;

› the general nature of the *relevant customer*'s client base, e.g., whether institutional or private client;

› the nature of the services that the *relevant customer* provides to its clients;

- the extent to which the *relevant customer* carries on business with its clients on a non-face to face basis or clients are otherwise subject to *enhanced CDD measures*; and
- the extent to which clients of the relevant *customer* may be PEPs or present a higher risk of *money laundering*, the *financing of terrorism*, or the financing of proliferation, and the sources of funds of such PEPs.

13. Immediately before applying the exemptions set out in Article 17B(1) of the *Money Laundering Order*, a *supervised person* may demonstrate that it has had regard for the higher risk of *money laundering,* the *financing of terrorism,* and the *financing of proliferation* should a *relevant customer* fail to apply *identification measures*, keep records, or keep records for the required period where it considers the following factors:

- the stature and regulatory track record of the *relevant customer*;
- the adequacy of the framework to combat *money laundering,* the *financing of terrorism,* and the *financing of proliferation* (including *targeted financial sanctions*) in place in the country or territory in which the *relevant customer* is based and the period of time that the framework has been in place;
- the adequacy of the supervisory regime to combat *money laundering,* the *financing of terrorism,* and the *financing of proliferation* to which the *relevant customer* is subject;
- the adequacy of *identification measures* applied by the relevant *customer* to combat *money laundering*, the *financing of terrorism*, and the financing of proliferation;
- the extent to which the *relevant customer* itself relies on other *obliged persons* to identify its clients and to hold evidence of identity, and whether such parties are *supervised persons* or carry on an *equivalent business*.

14. A *supervised person* may demonstrate that it has considered the adequacy of *identification measures* applied by a *relevant customer* where it takes one or more of the following steps:

- reviews its previous experience (if any) with the *relevant customer*;
- makes specific enquiries, e.g., through use of a questionnaire;
- reviews relevant policies and procedures of the relevant *customer*;
- where the *relevant customer* is a member of a *financial group*, makes enquiries concerning the extent to which group standards are applied to and assessed by the group's internal audit function;
- conducts (or commissions from an external expert) sample testing of the adequacy of the *relevant customer*'s *policies and procedures* to combat *money laundering,* the *financing of terrorism,* or the *financing of proliferation*, whether through onsite visits, or through requesting specific *CDD* information and/or copy documentation to be provided.

8.1.3 *CDD* requirements under Article 17B exemption

15. Article 17B of the *Money Laundering Order* can be applied to the same *customer* relationship, as they apply to separate identification requirements, however there are some elements of *CDD* that the *supervised person* will always be required to undertake – see the tables below:

CDD **element**	**Always required to be undertaken by the *supervised person***	
Identification measures	Risk assessment.	
	Obtain information on purpose/nature.	
Identification measures	Identify *customer.*	
	Identify person acting for *customer.*	Verify authority to act.
	Where *customer* is not an individual:	Understand ownership/control structure.
		Identify *Beneficial owners and/or controllers.*
Ongoing monitoring	Scrutinising transactions/activity.	
	Keep documents/information up to date.	
CDD **element**	**Articles 17B-D of the *Money Laundering Order* provide an exemption from this obligation**	
Identification measures	Identify third parties.	

16. Articles 17B of the *Money Laundering Order* **can** be applied to third parties which would, for example, encompass the investors in a limited partnership or a unit trust.

8.2 Exemption from applying *third party identification requirements* in relation to certain *relevant customers* involved in unregulated or non-public funds, *Trust Company Business* or the legal profession (Article 17C & 17D)

Statutory requirements (paraphrased wording)

17. *Under Article 17C(1) of the Money Laundering Order a relevant person is exempt from applying third party identification requirements in relation to a third party for which a relevant customer is acting if the relevant customer:*

a) *is, or carries on business in respect of, an unregulated fund, within the meaning of the [Collective Investment Funds (Unregulated Funds) (Jersey) Order 2008](), or equivalent business;*

b) *is, or carries on business in respect of, a fund that is a non-public fund, being a fund in respect of which a service is provided that is described in paragraph 9 of Part 2 of* Schedule 2 *to the Proceeds of Crime Law, or equivalent business;*

c) *carries on Trust Company Business and is registered to carry on such business under the FS(J) Law, or equivalent business, but only if the relevant person is:*

   i. *carrying on deposit-taking business;*

   ii. *a Lawyer carrying on business described in paragraph 21 of Part 3 of* Schedule 2 *to the Proceeds of Crime Law; or*

   iii. *an Accountant carrying on a business described in paragraph 22 of Part 3 of* Schedule 2 *to the Proceeds of Crime Law; or*

d) *is an independent legal professional carrying on a business described in paragraph 21 of Part 3 of* Schedule 2 *to the Proceeds of Crime Law and is registered to carry on such business under the Supervisory Bodies Law, but only if the relevant person is carrying on deposit-taking business.*

18. *Under Article 17C(2) of the Money Laundering Order, a relevant person who, by virtue of Article 17C(1) of the Money Laundering Order, does not apply third party identification requirements must:*

a) *be satisfied, by reason of the nature of the relationship with the relevant customer, that there is little risk of money laundering occurring; and*

b) *obtain adequate assurance in writing from the relevant customer that the relevant customer:*

i. *has applied the identification measures specified in Article 3(2)(b)of the Money Laundering Order to the third party, or if the relevant customer is not in Jersey, has applied similar identification measures that would satisfy the requirements in recommendations 10 and 12 of the FATF Recommendations;*

ii. *will provide the relevant person, without delay and in writing, with the information obtained from applying the identification measures, if so requested by the relevant person;*

iii. *will keep the evidence obtained during the course of applying the identification measures; and*

iv. *will provide the relevant person with that evidence without delay, if requested to do so by the relevant person.*

19. *Under Article 17C(3) of the Money Laundering Order the following requirements to adequate assurance apply:*

a) *assurance is adequate if it is reasonably capable of being regarded as reliable and the person who relies on it is satisfied that it is reliable;*

b) *assurance may be given in relation to one or more business relationships and for more than one transaction; and*

c) *assurance need not be given before deciding not to comply with third party requirements if an assurance has previously been given by that customer to the relevant person in relation to a business relationship or transaction.*

20. *Article 17C(4) of the Money Laundering Order provides that a relevant person (including a person who was formerly a relevant person) who has given an assurance to another person under Article 17C(2)(b) (or under an equivalent provision that applies outside Jersey) may, if requested by the other person, provide the person with the information or evidence obtained from applying the identification measures referred to in Article 17C(2)(b)(i) of the Money Laundering Order (see paragraph 147 above).*

Guidance notes

21. In relation to the exemption set out at Article 17C(1)(a) or (b) of the *Money Laundering Order*, a *supervised person* may be satisfied that there is little risk of *money laundering,* the *financing of terrorism,* or the *financing of proliferation* occurring where a particular fund is closed-ended, has no liquid market for its units, and permits subscriptions and redemptions to come from and be returned only to unitholders.

22. In relation to the exemption set out at Article 17C(1)(c)(i) of the *Money Laundering Order*, a *supervised person* may be satisfied that there is little risk of *money laundering,* the *financing of terrorism,* or the *financing of proliferation* occurring where:

- deposited funds are held only temporarily for one or more third parties in a client account operated by a person carrying on *Trust Company Business*, pending the transfer to a designated account for a third party, where the funds are not to be held on an undisclosed basis for longer than 40 days;
- deposited funds are held only temporarily for one or more third parties in a client account operated by a person carrying on *Trust Company Business*, pending the receipt of instructions when exiting a *customer* relationship, where the funds are not to be held on an undisclosed basis for longer than 40 days;
- deposited funds are held only temporarily for one or more third parties in a client account operated by a person carrying on *Trust Company Business*, to facilitate ad hoc (not routine) cheque payments where designated accounts do not otherwise have this facility;
- deposited funds are held only temporarily for one or more third parties in a client account operated by a person carrying on *Trust Company Business*, to facilitate the aggregation of statutory fees for onward payment;
- deposited funds are held only temporarily for one or more third parties in a client account operated by a person carrying on *Trust Company Business*, to receive fees payable to the *customer* which have been paid in advance;
- deposited funds are held only temporarily for one or more third parties in a client account operated by a person carrying on *Trust Company Business*, to receive *customer* money on an ad hoc basis paid to the *customer* in error;
- deposited funds are held for one or more third parties in a client account operated by a person carrying on *Trust Company Business*, where the number and value of third party transactions effected is low, e.g., to provide third parties with access to low-cost banking facilities where third parties' liquid assets are of insufficient value and volume for the establishment of a *Designated relationship* (e.g., balances of £1,000 or less per relationship, with little activity); or
- deposited funds are aggregated by a person carrying on *Trust Company Business* in order to attract a better return on investment for third parties, and where the aggregated deposit is received from and paid back (including income or profit generated) to an account held with another person carrying on deposit-taking business who is registered to do so by the *JFSC*, the Guernsey Financial Services Commission or the Isle of Man Financial Services Authority.

23. In relation to the exemption set out at Article 17C(1)(d) of the *Money Laundering Order*, a *supervised person* may be satisfied that there is little risk of *money laundering,* the *financing of terrorism,* or the *financing of proliferation* occurring where the deposit is in respect of a third party's registered contract within the meaning of the *Control of Housing and Work (Jersey) Law 2012*.

24. In relation to the exemptions set out at Article 17C(1)(c)(ii) and (iii) of the *Money Laundering Order*, guidance on when a *supervised person* may be satisfied that there is little risk of *money laundering,* the *financing of terrorism,* or the *financing of proliferation* occurring is provided in sections 20.4.1 and 21.3.4 of *this Handbook*.

8.2.1 Assessment of risk (Article 17D)

Overview

25. The risk factors that are set out in this section will also be relevant to a *CRA* that is conducted under section 3.3.4.1 of *this Handbook* in the cases highlighted at sections 4.3 and 4.5 of *this Handbook*.

Statutory requirements (paraphrased wording)

26. *Immediately before applying the exemptions set out in Article 17C, Article 17D(2) of the Money Laundering Order requires a relevant person to conduct an assessment as to whether it is appropriate to do so, having regard to the relevant customer's business and the higher risk of money laundering should the relevant customer fail to:*

- *apply the necessary identification measures to its customer(s); or*
- *keep records, or keep them for the period required to be kept.*

27. *Article 17D(2) of the Money Laundering Order requires a relevant person to prepare a written record of the reason why it is appropriate to apply CDD exemptions.*

28. *Article 17D(3) of the Money Laundering Order also sets out testing requirements for application of CDD exemptions under Article 17C of the Money Laundering Order. Under Article 17D(3) a relevant person must, in the manner, and as often as, the relevant person considers appropriate in all the circumstances, conduct tests in order to establish whether the relevant customer:*

a) *has appropriate policies and procedures in place to apply the identification measures described in Articles 13(1)(a), 13(1)(c)(ii) and 15 of the Money Laundering Order (or if the relevant customer is not in Jersey, similar identification measures that satisfy the FATF Recommendations in respect of identification measures);*

b) *obtains information in relation to the third party;*

c) *keeps the information or evidence that has been obtained in relation to the third party; and*

d) *provides the relevant person with that information or evidence without delay, if requested to do so by the relevant person.*

In conducting such tests, the relevant person must consider whether the relevant customer may be prevented, by application of a law, from providing that information or evidence.

29. *If, as a result of conducting the tests referenced above, the relevant person is unable to establish that the relevant customer complies with the above requirements under Article 17D (3)(b), (c) or (d) of the Money Laundering Order, the relevant person must immediately apply the identification measures specified in Article 13(1)(a) and 13(1)(c)(ii) of the Money Laundering Order.*

AML/CFT/CPF Codes of Practice

[COP75] In a case where, for a particular *business relationship*, testing under Article 17D(3) of the *Money Laundering Order* highlights that a *relevant customer* has not found out information or obtained evidence of identity for a third party (or parties), does not keep that information or evidence of identity, or will not provide it on request and without delay when requested to do so, a *supervised person* must review the basis upon which it has applied *CDD* exemptions to other relationships with that particular *relevant customer* (if any) to determine whether it is still appropriate to apply those measures.

Guidance notes

30. Immediately before applying the exemptions set out in Article 17C of the *Money Laundering Order*, a *supervised person* may demonstrate that it has had regard to a *relevant customer*'s business where it considers the following factors:

- the general risk appetite of the *relevant customer*;
- the geographic location of the *relevant customer*'s client base;
- the general nature of the *relevant customer*'s client base, e.g., whether institutional or private client;
- the nature of the services that the *relevant customer* provides to its clients;
- the extent to which the *relevant customer* carries on business with its clients on a non-face to face basis or clients are otherwise subject to *enhanced CDD measures*; and
- the extent to which clients of the relevant *customer* may be PEPs or present a higher risk of *money laundering*, the *financing of terrorism*, or the financing of proliferation, and the sources of funds of such PEPs.

31. Immediately before applying the exemptions set out in Article 17C of the *Money Laundering Order*, a *supervised person* may demonstrate that it has had regard for the higher risk of *money laundering,* the *financing of terrorism,* and the *financing of proliferation* should a *relevant customer* fail to apply *identification measures*, keep records, or keep records for the required period where it considers the following factors:

- the stature and regulatory track record of the *relevant customer*;
- the adequacy of the framework to combat *money laundering,* the *financing of terrorism,* and the *financing of proliferation* (including *targeted financial sanctions*) in place in the country or territory in which the *relevant customer* is based and the period of time that the framework has been in place;
- the adequacy of the supervisory regime to combat *money laundering,* the *financing of terrorism,* and the *financing of proliferation* to which the *relevant customer* is subject;
- the adequacy of *identification measures* applied by the relevant *customer* to combat *money laundering*, the *financing of terrorism*, and the financing of proliferation;
- the extent to which the *relevant customer* itself relies on other *obliged persons* to identify its clients and to hold evidence of identity, and whether such parties are *supervised persons* or carry on an *equivalent business*.

32. A *supervised person* may demonstrate that it has considered the adequacy of *identification measures* applied by a *relevant customer* where it takes one or more of the following steps:

- reviews its previous experience (if any) with the *relevant customer*;
- makes specific enquiries, e.g., through use of a questionnaire;
- reviews relevant policies and procedures of the relevant *customer*;
- where the *relevant customer* is a member of a *financial group*, makes enquiries concerning the extent to which group standards are applied to and assessed by the group's internal audit function;
- conducts (or commissions from an external expert) sample testing of the adequacy of the *relevant customer*'s *policies and procedures* to combat *money laundering,* the *financing of terrorism,* or the *financing of proliferation*, whether through onsite visits, or through requesting specific *CDD* information and/or copy documentation to be provided.

8.2.2 *CDD* requirements under Article 17C-D exemption

33. Article 17C-D of the *Money Laundering Order* can be applied to the same *customer* relationship, as they apply to separate identification requirements, however there are some elements of *CDD* that the *supervised person* will always be required to undertake – see the tables below:

<table>
<tr><th>CDD element</th><th colspan="2">Always required to be undertaken by the supervised person</th></tr>
<tr><td rowspan="2">Identification measures</td><td colspan="2">Risk assessment.</td></tr>
<tr><td colspan="2">Obtain information on purpose/nature.</td></tr>
<tr><td rowspan="4">Identification measures</td><td colspan="2">Identify customer.</td></tr>
<tr><td>Identify person acting for customer.</td><td>Verify authority to act.</td></tr>
<tr><td rowspan="2">Where customer is not an individual:</td><td>Understand ownership/control structure.</td></tr>
<tr><td>Identify Beneficial owners and/or controllers.</td></tr>
<tr><td></td><td colspan="2"></td></tr>
<tr><td rowspan="2">Ongoing monitoring</td><td colspan="2">Scrutinising transactions/activity.</td></tr>
<tr><td colspan="2">Keep documents/information up to date.</td></tr>
</table>

***CDD* element**	**Articles 17B-D of the *Money Laundering Order* provide an exemption from this obligation**
Identification measures	Identify third parties.

34. Articles 17C-D of the *Money Laundering Order* **can** be applied to third parties which would, for example, encompass the investors in a limited partnership or a unit trust.

8.3 Further exemptions from applying identification requirements

Statutory requirements (paraphrased wording)

35. *Article 18 of the Money Laundering Order provides further specific circumstances where exemptions from applying identification measures may be used.*

Insurance Business

36. *Under Article 18(1) of the Money Laundering Order, a relevant person is exempt from applying the identification measures specified in Article 13of the Money Laundering Order in respect of insurance business if:*

a) in the case of a policy of insurance in connection with a pension scheme taken out by virtue of a person's contract of employment or occupation, the policy contains no surrender clause and may not be used as collateral security for a loan;

b) a premium is payable in one instalment of an amount not exceeding £1,750; or

c) a periodic premium is payable and the total amount payable in respect of any calendar year does not exceed £750.

Pension, superannuation, employee benefit, share option or similar scheme

37. *Under Article 18(2) of the Money Laundering Order, a relevant person is exempt from applying the identification measures specified in Article 13 of the Money Laundering Order if:*

a) the business relationship or one-off transaction relates to a pension, superannuation, employee benefit, share option or similar scheme;

b) the contributions to the scheme are made by an employer or by way of deductions from wages;

c) the rules of the scheme do not permit the assignment of an interest of a member of the scheme except after the death of the member; and

d) the interest of a deceased member of the scheme is not being assigned.

Regulated person and those carrying on equivalent business

38. *Under Article 18(3) of the Money Laundering Order, a relevant person is exempt from applying the identification requirements in Article 13 of the Money Laundering Order in respect of the measures specified in Article 3(2)(a), (aa) and (c) of the Money Laundering Order in relation to a customer if the customer is:*

a) a regulated person;

b) a person who carries on equivalent business to any category of regulated business; or

c) a person wholly owned by a person (the "parent") mentioned in sub-paragraph (a) or (b), but only if:

i. the person is incorporated or registered in the same jurisdiction as the parent;

ii. the person has no customers who are not customers of the parent, the person's activity is ancillary to the regulated business or equivalent business carried on by the parent;

iii. *in relation to that activity, the person maintains the same policies and procedures as the parent.*

Public authority or body corporate/limited liability company with listed securities

39. *Under Article 18(4) of the Money Laundering Order, a relevant person is exempt from applying the identification requirements in Article 13 of the Money Laundering Order in respect of the measures specified in Article 3(2)(a) and 3(2)(aa) of the Money Laundering Order (in so far as those measures require identifying any person purporting to act on behalf of the customer), 3(2)(c)(ii) and 3(2)(c)(iii) of the Money Laundering Order in relation to a customer if the customer is:*

a) *a public authority acting in that capacity;*

b) *a body corporate or limited liability company the securities of which are listed on an IOSCO-compliant market or on a regulated market; or*

c) *a person wholly owned by a person mentioned in sub-paragraph (b).*

Person authorised to act on behalf of customer

40. *Under Article 18(5) of the Money Laundering Order, a relevant person is exempt from applying the identification requirements in Article 13of the Money Laundering Order in respect of the measures specified in Article 3(2)(aa) of the Money Laundering Order (in so far as those measures require identifying any person purporting to act on behalf of a customer) in relation to a person if:*

a) *the person is authorised to act on behalf of the customer;*

b) *the customer is not a relevant person;*

c) *the person acts on behalf of the customer in the course of employment by a person carrying on a financial services business; and*

d) *the financial services business is a regulated business or an equivalent business to a regulated business.*

Specified business (Lawyers and real estate agents)

41. *Under Article 18(6) of the Money Laundering Order, a relevant person is exempt from applying the identification requirements in Article 13 of the Money Laundering Order to the extent that the measures require identification of a person within the meaning of Article 3(4)(b) of the Money Laundering Order if:*

a) *the relevant person's business falls within paragraph 21 [Lawyers] or 19 [Real estate agents] of Part 3 of* Schedule 2 *to the Proceeds of Crime Law; and*

b) *that person enters into a business relationship or carries out a one-off transaction for the purpose of enabling a customer, directly or indirectly, to enter into a registered contract (within the meaning of the [Control of Housing and Work (Jersey) Law 2012](#).*

AML/CFT/CPF Codes of Practice

[COP76] For each case described in Article 18 of the *Money Laundering Order*, a *supervised person* must obtain information on the purpose and intended nature of the business relationship or one-off transaction.

[COP77] A *supervised person* must obtain and retain documentation establishing that the *customer* is entitled to benefit from an exemption in Article 18 of the *Money Laundering Order*.

8.3.1 *CDD* requirements under Article 18 exemptions

42. Article 18 of the *Money Laundering Order* can be applied to the same *customer* relationship, as they apply to separate identification requirements, however there are some elements of *CDD* that the *supervised person* will always be required to undertake – see the tables below:

***CDD* element**	**Always required to be undertaken by the *supervised person***
Identification measures	Risk assessment.
	Obtain information on purpose/nature.
	Identify third parties.
Ongoing monitoring	Scrutinising transactions/activity.
	Keep documents/information up to date.

<table>
<tr><th>CDD element</th><th colspan="2">Article 18 of the Money Laundering Order provides an exemption from this obligation (N.B: Does not apply to third parties)</th></tr>
<tr><td rowspan="4">Identification measures</td><td colspan="2">Identify customer.</td></tr>
<tr><td>Identify person acting for customer.</td><td>Verify authority to act.</td></tr>
<tr><td rowspan="2">Where customer is not an individual:</td><td>Understand ownership/control structure.</td></tr>
<tr><td>Identify Beneficial owners and/or controllers.</td></tr>
</table>

43. Article 18 of the *Money Laundering Order* only applies to the *customer* and **does not** extend to third parties. For example, it would apply to a general partner of a limited partnership or a trustee of a trust, but not to the limited partnership or trust itself.

8.3.2 Pension, superannuation, employee benefit, share option or similar schemes

Overview

44. Where a *supervised person* enters into a *business relationship* or carries out a *one-off transaction* relating to a pension, superannuation, employee benefit, share option or similar scheme, in some limited circumstances there is no requirement to apply *identification measures*.

45. However, the exemption cannot be applied if a *supervised person* considers that there is a higher risk of *money laundering,* the *financing of terrorism,* or the *financing of proliferation*.

Guidance notes

46. A *supervised person* may demonstrate that it considers whether there is a higher risk of *money laundering,* the *financing of terrorism,* or the *financing of proliferation* when, among other things, it considers the reputation of the sponsoring employer and adequacy of controls in place over membership.

8.3.3 Jersey public authority

Overview

47. Where a *customer* is a *public authority* then, in line with Article 18(4)(a) of the *Money Laundering Order*, there is no requirement to apply *identification measures* on that *customer*, on the *Beneficial owners and/or controllers* of the *customer*, or those purporting to act on behalf of the *customer*.

48. However, in the above scenario the obligation to apply *identification measures* to any third party for which the *customer* may be acting and to verify the authority of persons acting on behalf of the *customer* remain in force.

49. The following may be considered to be public authorities in Jersey:

- a government department of the States of Jersey;
- a majority States-owned company;
- an agency established by a law of the States of Jersey;
- a parish authority.

8.3.4 Body Corporate/*limited liability company* with listed securities

Overview

50. Where a *customer* is a body corporate or *limited liability company*, the securities of which are listed on a market that conforms to international standards set by *IOSCO* or on a *regulated market*, then in line with Article 18(4)(b) of the *Money Laundering Order*, there is no requirement to apply *identification measures* on that *customer* (or any wholly owned subsidiary), on the *Beneficial owners and/or controllers* of the *customer* (or any wholly owned subsidiary), or those purporting to act on behalf of the *customer* (or any wholly owned subsidiary).

51. However, in the above scenario the obligations to apply *identification measures* to any third party for which the *customer* (or wholly owned subsidiary) may be acting and to verify the authority of persons acting on behalf of the *customer* (or wholly owned subsidiary) remain in force.

52. A market may be considered to be *IOSCO*-compliant if it is operated in a country or territory that has been assessed as having “fully implemented” or “broadly implemented” *IOSCO* Principles 16 and 17. In order to be assessed as having “fully implemented” or “broadly implemented” Principle 17, a country or territory must require:

- information about the identity and holdings of persons who hold a substantial *beneficial ownership* interest to be disclosed on a timely basis;
- material changes in such ownership and other required information to be disclosed in a timely manner.

53. Whilst there is not a global list of countries and territories that “fully implement” or “broadly implement” *IOSCO* Principles 16 and 17, reference may be made to *IMF* Financial System Stability Assessment reports, prepared as part of the *IMF* Financial Sector Assessment Program.

54. Guidance published by the UK’s Joint *Money Laundering* Steering Group addresses what may be considered to be a *regulated market*. The only list of exchanges currently available is for *EU-regulated market*s (follow the link provided in the glossary entry for *regulated market*).

8.3.5 Regulated persons and those carrying on equivalent business

Overview

55. Where a *customer* is:

- a regulated person (defined in Article 1(1) of the *Money Laundering Order*);
- a person who carries on *equivalent business* to any category of *regulated business*; or
- wholly owned by a person listed above and which fulfils certain conditions (see Article 18(3)(c) of the *Money Laundering Order*)

Then in line with Article 18(3) of the *Money Laundering Order*, there is no requirement to apply *identification measures* in respect of the *customer*, the *Beneficial owners and/or controllers* of the *customer*, or those purporting to act on behalf of the *customer*. Nor is there a requirement to verify the authority of any person purporting to act for the *customer*.

56. However, these provisions do not also provide an exemption in respect of any third party (or parties) for whom the *customer* is acting, or for the *Beneficial owners and/or controllers* of such a third party (or parties).

8.3.6 Person authorised to act on behalf of a *customer*

Guidance notes

57. Where a person authorised to act on behalf of a *customer* holds their role by virtue of their employment by (or position in) a business that is a *regulated person* or an equivalent *regulated business*, a *supervised person* may demonstrate that this exemption applies where it obtains:

- the full name of the individual; and
- an assurance from the employer that the individual is an officer or employee.

8.3.7 Jersey property transfers

Overview

58. This section relates to the exemption available under Article 18(6) of the *Money Laundering Order*, which provides that a *supervised person* that is a *Lawyer* or a *real estate agent*, which enters into a *business relationship* or carries out a *one-off transaction* for the purpose of enabling a *customer*, directly or indirectly, to enter into a registered contract within the meaning of the Control of Housing and Work (Jersey) Law 2012 (i.e. where it is to be passed before the Royal Court and registered in the Public Registry of Contracts), need not obtain **evidence of identity** of its *customer*. See also section 20.4.2.

AML/CFT/CPF Codes of Practice

[COP78] For each case described in Article 18 of the *Money Laundering Order*, a *supervised person* must obtain information on the purpose and intended nature of the *business relationship* or *one-off transaction*.

[COP79] A *supervised person* that is a *lawyer* or *real estate agent* must obtain and retain documentation establishing that its *customer* is entitled to benefit from the exemption set out in Article 18(6) of the *Money Laundering Order*.

8.3.8 Exemption from applying *third party identification requirements* in relation to certain *relevant customers* involved in *Trust Company Business*

59. This section is supplemental to and should be read in conjunction with section 20.4.1 and 21.3.4 of *this Handbook*.

60. Article 17C(1)(c)(ii) of the *Money Laundering Order* provides that a *supervised person* that is a *Lawyer/Accountant* is exempt from applying third party identification requirements in relation to a third party for which a relevant *customer* is acting if the relevant *customer* carries on Trust Company Business and is registered to carry on such business under the FS(J) Law, or equivalent business.

61. Article 17C(2) of the *Money Laundering Order* requires that a *supervised person* who does not apply *third party identification requirements* must be satisfied, by reason of the nature of the relationship with the *relevant customer*, that there is little risk of *money laundering, terrorism financing* , or *proliferation financing* occurring.

8.4 Exemptions from *CDD* requirements where there is outsourcing or an *AMLSP* is appointed

62. Exemptions from *CDD* requirements can still be used by *supervised person*s where their *customer* is a *supervised person* in receipt of outsourced services and/or *AMLSP* services:

- Can a *supervised person* using an Outsourced service provider/*AMLSP* still use the exemptions even if the *AMLSP*/outsourced service provider is applying *CDD* measures on their behalf? Yes, subject to consideration of criteria of exemption and Article 17A of the *Money Laundering Order*;
- Can another *supervised person* (*Supervised person* 1) with a *Supervised person* 2 as their *customer*, where *Supervised person* 2 is using an outsourced service provider/*AMLSP* (who will apply *CDD* measures for *Supervised person* 2 as part of the outsourced services/*AMLSP*) apply exemptions from *CDD* measures to that *Supervised person*? Yes, subject to consideration of criteria of exemption and Article 17A of the *Money Laundering Order*;
- Can an outsourced service provider/*AMLSP* apply Article 18 of the *Money Laundering Order* identification exemptions to the *customer* of the *supervised person* on its own behalf? No, A *customer* relationship with a *supervised person* does not create a *customer* relationship with the *AMLSP* or the outsourcing service provider;
- Can an outsourced service provider/*AMLSP* contracted to provide *CDD* measures for the *supervised person* apply Article 17 of the *Money Laundering Order* third party identification exemptions to the *customer*s of the *supervised persons* or the third parties for whom they act*?* The *JFSC* would not expect the *AMLSP or* outsourcing service provider to apply Article 17 of the *Money Laundering Order* third party identification exemptions to the *customer*s of the *supervised persons* or the third parties for whom they act to avoid undertaking its contractual obligations to apply *CDD* measures as *AMLSP or* outsourcing service provider on behalf of that *supervised person.*

8.5 Simplified *identification measures* – Obtaining evidence of identity for very low risk products/services

Overview

63. Where funds involved in a *business relationship*:

- have been received from a bank that is a *regulated person* or carries on *equivalent business* to deposit-taking (see section 1.8 of *this Handbook* regarding *equivalent business*); and

- have come from an account in the sole or joint name of the *customer* who is an individual (or are individuals);

Then the receipt of funds from such an account may be considered to be reasonably capable of verifying that the person to be identified is who they are said to be where the product or service requested by the *customer* is considered to present a very low risk of *money laundering,* the *financing of terrorism,* or the *financing of proliferation*. This will be the case where funds may only be received from, and paid to, an account in the *customer's* name, i.e., a product or service where funds may not be paid in by, or paid out to, external parties.

64. In the event that any of the conditions set below are breached, evidence of identity for the *customer* must be obtained at that time in accordance with section 4 of *this Handbook* and this section 7 of *this Handbook*.

AML/CFT/CPF Codes of Practice

[COP80] The concession referred to above must not be applied in the following circumstances:

- where a *supervised person* suspects *money laundering*, the *financing of terrorism*, or the financing of proliferation;
- in any situation which by its nature can present a higher risk of *money laundering*, the *financing of terrorism*, or the financing of proliferation;
- where the *customer* has a relevant connection to an enhanced risk state; or
- where the *customer* is resident in a country or territory that is not compliant with the FATF Recommendations.

[COP81] To benefit from the concession, the product or service must satisfy the following conditions:

- all initial and future payments must be received from an account at a bank that is a *regulated person* or carries on an equivalent business to deposit-taking (see section 1.8 of *this Handbook*), where the account can be confirmed as belonging to the *customer*;
- *no* initial or future payments may be received from external parties;
- cash withdrawals are not permitted, with the exception of face-to-face withdrawals by the *customer*, where they are required to produce evidence of identity before the withdrawal can be made;
- no payments may be made, other than to an account at a bank that is a *regulated person* or carries on an *equivalent business* to deposit-taking (see section 1.8 of *this Handbook*), where the account can be confirmed as belonging to the *customer*, or on the death of the *customer* to a personal representative named in the grant of probate or the letters of administration; and
- no future changes must be made to the product or service that enable funds to be received from or paid to external parties.

[COP82] A *supervised person* must obtain and retain evidence confirming that payment has been received from an account at a bank that is a *regulated person* or carries on an *equivalent business* to deposit-taking (see section 1.8 of *this Handbook*), and, where a request for a withdrawal or transfer to another bank account is received, confirmation that this account is also in the *customer*'s name and held at a bank that is a *regulated person* or carries on an *equivalent business* to deposit-taking.

[COP83] If a *supervised person* has reason to suspect that the motive behind a particular transaction, or the way a business is being structured, is to avoid standard *identification measures*, it must not use this concession.

9 REPORTING *MONEY LAUNDERING,* THE *FINANCING OF TERRORISM* OR *PROLIFERATION,* AND SANCTIONS REPORTING OBLIGATIONS

9.1 Overview of section

1. Under the *Proceeds of Crime Law* and *Terrorism Law*, where any *supervised person* conducting *supervised business* in or from within Jersey knows or suspects or has reasonable grounds for knowing or suspecting that another person is engaged in *money laundering* or the *financing of terrorism*, then it must report its knowledge or suspicion to the *FIU*.

2. Under the *Money Laundering Order*, a *supervised person* must have procedures in place for reporting such knowledge or suspicion of *money laundering* or the *financing of terrorism* activity to the *FIU*.

3. This section outlines the statutory provisions concerning reporting that apply to:

› an *Employee of a supervised person*; and

› a *supervised person*, in the course of carrying on any trade, profession or business.

It also sets *AML/CFT/CPF Codes of Practice* for and provides guidance to:

› *Employees* making a report to their *MLRO* (or *Deputy MLRO*) (referred to as an internal *SAR*); and

› *MLROs* (and *Deputy MLROs*) making a report to the *FIU* (referred to as an external *SAR*).

4. This section also considers the consent that must be sought from the *FIU* before proceeding with a transaction or continuing a *business relationship*, and the application of tipping off provisions.

5. An important precondition for making a *SAR* is to know enough about a *business relationship* or *one-off transaction* to be able to recognise what is “unusual”. Such knowledge is dependent upon the application of *identification measures* and ongoing monitoring.

6. A *SAR* may also be based on information from other sources, including law enforcement agencies, other government bodies, the media, or the *customer*.

7. Whilst this section describes reports made to the *FIU* under the *Proceeds of Crime Law* and *Terrorism Law* as *SARs*, depending on the circumstances such reports may involve **knowledge** of *money laundering* or the *financing of terrorism*, rather than **suspicion** (or reasonable grounds for knowledge or suspicion).

8. Section 9.8 of *this Handbook* explains the separate sanctions compliance reporting obligations under the *Sanctions and Asset-Freezing Law*.

9.2 Reporting knowledge or suspicion

Overview

9. Legislation deals with reporting by a *supervised person* and employees in the course of carrying on a *supervised business* in two ways:

› there is a **reporting requirement** under Article 34D of the *Proceeds of Crime Law* and Article 21 of the *Terrorism Law* - a *SAR* must be made when there is knowledge, suspicion, or reasonable grounds for suspecting that:

  - another person is engaged in *money laundering* or the *financing of terrorism*; or
  - any property constitutes or represents proceeds of criminal conduct; or
  - any property has been, is being or is intended to be used in criminal conduct; or
  - any property is or may be terrorist property.

› there is **protection for reporting** under Article 32 of the *Proceeds of Crime Law* and under Article 18 of the *Terrorism Law* when there is suspicion or belief that any property constitutes or represents:

  - the proceeds of criminal conduct; or
  - property used in or intended to be used in criminal conduct; or
  - terrorist property.

› Where the person making the report does any act or deals with the property in any way which would otherwise amount to the commission of a *money laundering* or the *financing of terrorism* offence, the person shall not be guilty of that offence (where certain conditions are fulfilled in section 9.2.2 of *this Handbook*) where it makes a **protective report**.

10. In practice, a report made in accordance with the **reporting requirement** will also provide **protection**. For example, where a *supervised person* knows or suspects, or has reasonable grounds for knowing or suspecting, that property constitutes or represents the proceeds of criminal conduct (or has been, is being or is intended to be used in criminal conduct), and has possession of that property, it must report its knowledge or suspicion under Article 34D of the *Proceeds of Crime Law*. Where it makes such a report, this will also address its suspicion or belief that property constitutes or represents the proceeds of criminal conduct (or has been used in or is intended to be used in criminal conduct) under Article 32 of the *Proceeds of Crime Law*. The effect of this is that the *supervised person* does not commit a *money laundering* offence under Article 30 (and potentially Article 31) of the *Proceeds of Crime Law.*

11. Within the *Proceeds of Crime Law* there is also a **reporting requirement** (Article 34A) and **protection for reporting** (Article 32) in a case where a matter or information comes to a *supervised person's* attention other than in the course of carrying on a *supervised business* (i.e., through any trade, profession, business, or employment). A similar **reporting requirement** (and **protection**) may also be found in Articles 19 and 18 of the *Terrorism Law*. This is different to the aforementioned requirement at Article 34D of the *Proceeds of Crime Law*, where the matter or information comes to a person's attention in the course of carrying on a *financial services business* (i.e., a *supervised business*).

12. Whilst the *Proceeds of Crime Law* and *Terrorism Law* anticipate that a report may be made by an *Employee* directly to the *FIU*, Article 21 of the *Money Laundering Order* requires that such reporting is made in line with a *supervised person's* **reporting procedures**. Such procedures must ensure that a report by an employee is made to the *MLRO* (or *Deputy MLRO*).

13. Where the *MLRO* (or *Deputy MLRO*) resolves to make an external *SAR* as a result of an internal *SAR* made under the *Proceeds of Crime Law* or *Terrorism Law*, Article 21 of the *Money Laundering Order* requires that *SAR* to be made using the approved form. In this section "approved form" means the form approved by *the Minister*, which may be changed from time to time.

14. Where an external *SAR* is made using the approved form to the *FIU*, in the circumstances where a *supervised person* is also subject to the requirements of the EU Legislation (Information Accompanying Transfers of Funds) (Jersey) Regulations 2017 (as amended) and is transacting with group counterparties, an external *SAR* should also be made in each jurisdiction to which the transaction relates. This external *SAR* is in addition to any made to the *FIU* and can be made either by the *supervised person*, or the group counterparty who was also subject to the same transaction in that jurisdiction.

15. A *SAR* made in respect of a *business relationship* or *one-off transaction* does not remove the need to make **further reports** in respect of knowledge or suspicion that subsequently arises in respect of that *business relationship* or *one-off transaction* (which may also be a series of linked transactions).

9.2.1 Requirement to report knowledge or suspicion

Overview

16. While carrying on a *supervised business*, *Employees* of a *supervised person* are required to raise an internal *SAR* **as soon as practicable** where they have knowledge or suspicion, or where there are reasonable grounds for having knowledge or suspicion that:

› another person is engaged in *money laundering* or the *financing of terrorism*; or

› any property constitutes or represents the proceeds of criminal conduct; or

› any property has been, is being, or is intended to be used in criminal conduct; or

› any property is, or may be, terrorist property.

17. What may constitute reasonable grounds for knowledge or suspicion will be determined by the facts or circumstances present, from which an honest and reasonable *employee* working in a *supervised person* would have inferred knowledge or formed a suspicion (the so-called "objective test"). See section 9.2.3.3 of *this Handbook*.

18. Something which appears unusual is not necessarily suspicious but will likely be the cause for further investigation. This may, in turn, require judgement to be exercised as to whether something is indeed suspicious. The provisions under section 8.5 of *this Handbook* regarding tipping off may also need to be considered.

19. A *supervised person's MLRO* (or *Deputy MLRO*) must consider all internal *SARs* **as soon as practicable**.

20. A *supervised person's MLRO* (or *Deputy MLRO*) is required to make an external *SAR* **as soon as practicable** if they know, suspect, or have reasonable grounds for suspecting that:

› another person is engaged in *money laundering* or the *financing of terrorism*; or

› any property constitutes or represents the proceeds of criminal conduct; or

› any property has been, is being, or is intended to be used in criminal conduct; or

› any property is, or may be, terrorist property.

21. Guidance on how a *supervised person* may demonstrate that internal and external *SARs* are being made as soon as reasonably practicable is set out at sections 9.3.1 and 9.3.2 of *this Handbook*.

22. Once an *Employee* has made an internal *SAR* and provided any additional information that may be requested by the *MLRO* (or *Deputy MLRO*), they will have fully satisfied their statutory obligation in respect of the particular matter or information reported.

23. Under the *Proceeds of Crime Law*, the **requirement to report** applies in relation to the proceeds of such criminal conduct that constitutes an offence specified in Schedule 1 of the *Proceeds of Crime Law*, or, if it occurs or has occurred outside Jersey, would have constituted such an offence if it occurred in Jersey.

24. Under the *Terrorism Law,* the **requirement to report** applies in relation to property which is intended or likely to be used for the purposes of terrorism in Jersey or elsewhere, or for the support of a terrorist entity in Jersey or elsewhere.

25. Other than in the course of carrying on a *supervised business* (i.e. any other trade, profession or business carried on by the *supervised person*), *Employees* of a *supervised person* are also required to raise an internal *SAR* where they have knowledge or suspicion that another person is engaged in *money laundering* or the *financing of terrorism* - where information or a matter on which knowledge or suspicion is based comes to them **in the course of their employment**. This will apply irrespective of the underlying nature of the business that is carried on, and irrespective of whether the business is being carried out on behalf of another person, e.g., under an outsourcing arrangement.

26. Where an *MLRO* who is part of a group receives information relating to suspicious activities within that group but with no specific Jersey connection, such information is not considered to have come to the *MLRO* in the course of carrying on a *supervised business*. This means that such matters, in the absence of a specific Jersey connection, are not required to be reported.

Statutory requirements (paraphrased wording)

27. *Under Article 34D(4) of the Proceeds of Crime Law, a relevant person and Employees of that relevant person are required to make a report where two conditions are fulfilled.*

28. *The first is that they know, suspect or have reasonable grounds for suspecting that:*

- *another person is engaged in money laundering or the financing of terrorism;*
- *any property constitutes or represents the proceeds of criminal conduct; or*
- *any property has been, is being or is intended to be used in criminal conduct.*

29. *The second is that the information or matter on which the knowledge or suspicion is based, or which gives reasonable grounds for suspicion, comes to them in the course of the carrying on of a financial services business.*

30. *Such a report must be made to the FIU (or, in the case of an Employee, to the relevant person's MLRO (or Deputy MLRO)), delivered in good faith, and made as soon as is practicable after the information or other matter on which the knowledge or suspicion is based, or which gives reasonable grounds for suspicion, comes to their attention.*

31. *However, under Article 34D(5) of the Proceeds of Crime Law, a person does not commit an offence if they have a reasonable excuse for not disclosing the information or other matter, or the person is a professional legal adviser, and the information or other matter comes to them in the circumstances of legal privilege (except items held with the intention of furthering a criminal purpose).*

32. *Under Article 34D(6) of the Proceeds of Crime Law, an Employee of a relevant person does not commit an offence of failing to disclose if they have not been given material training and, as a result, did not know or suspect that the other person was engaged in money laundering or the financing of terrorism.*

33. *Under Article 34D(9) of the Proceeds of Crime Law, a report made to the FIU (or to the relevant person's MLRO or Deputy MLRO) shall not be treated as a breach of any restriction imposed by statute, contract or otherwise.*

34. *When considering a report made under the Proceeds of Crime Law or Terrorism Law, Article 21(2) and (3) of the Money Laundering Order states that, if the MLRO (or Deputy MLRO) knows or suspects, or has reasonable grounds for knowing or suspecting, that another person is engaged in money laundering or the financing of terrorism, they must report to the FIU as soon as is practicable using the approved form. Among other things, delivery of the approved form must comply with the requirements (including those in respect of delivery) indicated on the approved form.*

35. *Following the submission of a report, Article 21(4) of the Money Laundering Order requires a MLRO (or Deputy MLRO) to provide the FIU (within a set period of time) with such additional information relating to that report as may reasonably be requested.*

36. *A person who fails to make a report under Article 34D of the Proceeds of Crime Law is liable to imprisonment for a term not exceeding 5 years or to a fine or to both. An individual who fails to make a report using the approved form under Article 21(2) of the Money Laundering Order is liable to imprisonment for a term not exceeding 2 years or to a fine or to both. A body corporate who fails to make a report using the approved form under Article 21(2) of the Money Laundering Order is liable to a fine.*

37. *Article 34A of the Proceeds of Crime Law contains a similar requirement to report. In a case where a relevant person or employee knows or suspects that another person is engaged in money laundering or the financing of terrorism, and the information or other matter on which that knowledge or suspicion is based comes to their attention in the course of any trade, profession, business or employment (other than carrying on of a financial services business), they must report that knowledge or suspicion and information or other matter to the FIU (or, in the case of an employee, to the relevant person's MLRO (or Deputy MLRO)), in good faith and as soon as is practicable after the information or other matter comes to their attention.*

38. *Under Article 34A(3) of the Proceeds of Crime Law, a report made to the FIU (or to the relevant person's MLRO or Deputy MLRO) under Article 34A shall not be treated as a breach of any restriction imposed by statute, contract or otherwise.*

39. *Article 8 of the Money Laundering Order requires a relevant person to ensure that the MLRO (or Deputy MLRO) has timely access to all records that are necessary or expedient for the purpose of performing his or her functions as a reporting officer, including, in particular, the records that a relevant person must keep under Article 19 of the Money Laundering Order.*

40. *"Criminal conduct" is defined in Article 1(1) of the Proceeds of Crime Law as conduct that constitutes an offence specified in Schedule 1 of that law, or, if it occurs or has occurred outside Jersey, would have constituted such an offence if occurring in Jersey.*

41. *Articles 19 to 22 of the Terrorism Law contain similar reporting requirements in respect of the financing of terrorism.*

42. *In particular, Article 21 of the Terrorism Law requires a relevant person and Employee of that relevant person to make a report where two conditions are fulfilled.*

43. *The first is that they know, suspect or have reasonable grounds for suspecting that:*

- *another person is engaged in the financing of terrorism; or*
- *any property is, or may be, terrorist property.*

44. *The second is that the information or matter on which the knowledge or suspicion is based, or which gives reasonable grounds for suspicion, comes to them in the course of the carrying on of a financial services business.*

45. *Terrorist property is defined in Article 3 of the Terrorism Law to mean property, which is intended to be used, or likely to be used, for the purposes of terrorism or support of a terrorist entity. A terrorist entity is defined in Article 4 as an entity which commits, prepares or instigates an act of terrorism or facilitates the commission, preparation or instigation of an act of terrorism.*

46. *The meaning of "terrorism" is defined in Article 2 of the Terrorism Law. The meaning of "terrorist entity" is defined in Article 4 of the Terrorism Law.*

9.2.2 Protective report

Overview

47. In the course of carrying on its business, *Employees of a supervised person* will raise an internal *SAR* in order to be protected where they suspect or believe that:

- property constitutes or represents the proceeds of criminal conduct or property used in or intended to be used in criminal conduct; or
- property is terrorist property; or
- they are providing a service for the purposes of terrorism or for the support of a terrorist entity.

48. This will apply irrespective of the underlying nature of the business that is carried on, and irrespective of whether the business is being carried out on behalf of another person, e.g., under an outsourcing arrangement.

49. A *supervised person's MLRO* (or *Deputy MLRO*) must consider all internal *SARs* **as soon as practicable**.

50. Under the *Proceeds of Crime Law* and *Terrorism Law*, a *supervised person's MLRO* (or *Deputy MLRO*) is required to make an external *SAR* **before** the *supervised person* does a particular act, or **as soon as reasonably practicable** after the person has done the act or has become involved in the transaction or arrangement, to be protected.

51. In most cases, where the person making the report does any act or deals with the property in any way which would otherwise amount to the commission of a *money laundering* or the *financing of terrorism* offence, the person shall not be guilty of that offence where it makes such a protective report, and certain conditions are fulfilled.

52. Under the *Proceeds of Crime Law*, protection for reporting applies in relation to the proceeds of such criminal conduct that constitutes an offence specified in Schedule 1 of the *Proceeds of Crime Law*, or if it occurs or has occurred outside Jersey, would have constituted such an offence if occurring in Jersey.

53. Under the *Terrorism Law*, protection for reporting applies in relation to property which is intended or likely to be used for the purposes of terrorism in Jersey or elsewhere or for the support of a terrorist entity in Jersey or elsewhere.

Statutory requirements (paraphrased wording)

54. *Where a relevant person or Employee of a relevant person suspects or believes that any property constitutes or represents the proceeds of criminal conduct or property used in or intended to be used in criminal conduct and makes a report to the FIU (or to the relevant person's MLRO or Deputy MLRO) under Article 32 of the Proceeds of Crime Law, they will not have committed a money laundering offence if the report is made in good faith and either:*

- *if the report is made before the person does the act in question, the act is done with the consent of the FIU; or*
- *if the report is made after the person does the act in question, it is made on the person's own initiative and as soon as reasonably practicable after the person has done the act in question.*

55. *In proceedings against a person for an offence under Article 30 of the Proceeds of Crime Law, it shall be a defence under Article 32(7) to provide that the alleged offender intended to make a report and there is a reasonable excuse for the failure to have made a report.*

56. *Under Article 32(2) of the Proceeds of Crime Law, a report made to the FIU (or to the relevant person's MLRO or Deputy MLRO) under Article 32 of the Proceeds of Crime Law shall not be treated as a breach of any restriction imposed by statute, contract or otherwise, and shall not involve the person making it in liability of any kind.*

57. *When considering a report made under the Proceeds of Crime Law or Terrorism Law, Article 21(2) and (3) of the Money Laundering Order states that, if the MLRO (or Deputy MLRO) knows or suspects that another person is engaged in money laundering or the financing of terrorism, they must report to the FIU as soon as is practicable using the approved form. Among other things, delivery of the form must comply with the requirements (including those in respect of delivery) indicated on the form.*

58. *Left intentionally blank.*

59. *Left intentionally blank.*

60. *Subsequent to making a report, Article 21(4) of the Money Laundering Order requires a MLRO (or Deputy MLRO) to provide the FIU (within a set period of time) with such additional information relating to that report as may reasonably be requested.*

61. *An individual who fails to make a report using the approved form under Article 21(2) of the Money Laundering Order is liable to imprisonment for a term not exceeding 2 years or to a fine or to both. A body corporate who fails to make a report using the approved form under Article 21(2) of the Money Laundering Order is liable to a fine.*

62. *Article 8 of the Money Laundering Order requires a relevant person to ensure that the MLRO (or Deputy MLRO) has timely access to all records that are necessary or expedient for the purpose of performing their functions as a reporting officer, including, in particular, the records that a relevant person must keep under Article 19 of the Money Laundering Order.*

63. *"Criminal conduct" is defined in Article 1(1) of the Proceeds of Crime Law as conduct that constitutes an offence specified in Schedule 1 of the Proceeds of Crime Law, or, if it occurs or has occurred outside Jersey, would have constituted such an offence if occurring in Jersey.*

64. *Article 18 of the Terrorism Law contains similar provisions in circumstances where the financing of terrorism offences would otherwise be committed. In particular:*

- *Article 18(1) provides that no financing of terrorism offence is committed if a person is acting with the express consent of the FIU;*

- *Article 18(2) provides that no financing of terrorism offence is committed if a person discloses a suspicion or belief that property is terrorist property after they have become involved in a transaction or arrangement to the FIU in good faith and as soon as reasonably practicable;*
- *Article 18(3) provides that no financing of terrorism offence is committed if a person discloses a suspicion or belief to the FIU that a service is being, or is to be, provided for the purposes of terrorism or for the support of a terrorist entity, after they have become involved in a transaction or arrangement, in good faith and as soon as reasonably practicable.*

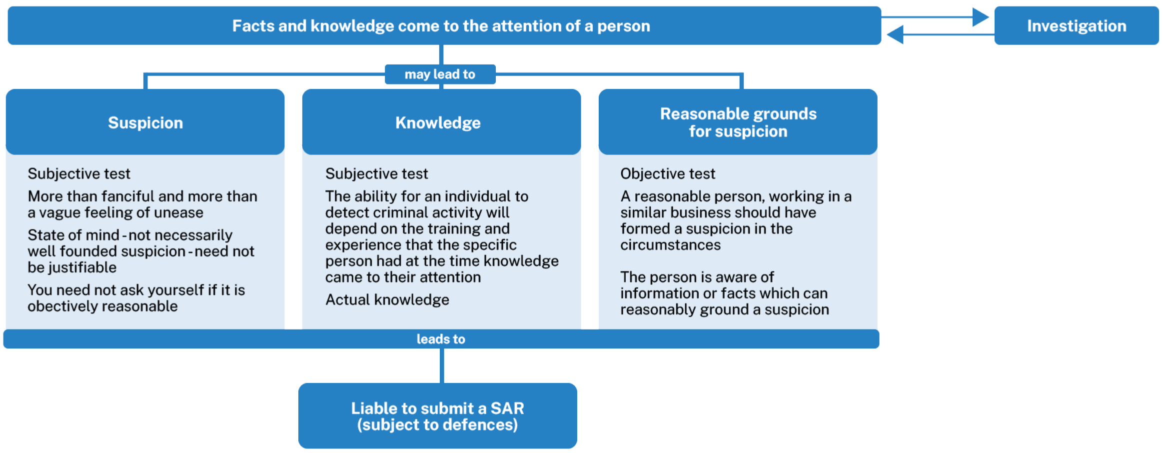
65. *However, unlike the Proceeds of Crime Law, an Employee who makes a report to the relevant person's MLRO (or Deputy MLRO) may still be charged with an offence. In such a case, it will be a defence under Article 18(8) of the Terrorism Law for the Employee to prove that a report was made in good faith and in accordance with the employer's procedures.*

9.2.3 What constitutes knowledge or suspicion?

Guidance notes

66. The terms 'knowledge', 'suspicion' and 'reasonable grounds for suspicion' are not defined within Jersey law. However, case law has provided some guidance on how they should be interpreted.

67. The diagram below summarises the differences between each of these three terms and where they sit within the wider reporting process:



9.2.3.1 **Knowledge**

68. Knowledge means actual knowledge. There is some suggestion that wilfully shutting one's eyes to the truth may amount to knowledge. However, the current general approach from the criminal courts is that nothing less than actual knowledge will suffice.

9.2.3.2 **Suspicion**

69. By contrast, suspicion is more than speculation, but it falls short of proof or knowledge. There is no requirement for the suspicion to be clear or firmly grounded on specific facts, but there must be a degree of satisfaction, not necessarily amounting to belief, but at least extending beyond speculation.

70. The test for whether a person holds a suspicion is subjective. The suspicion is one of believing that something is possible, which is more than fanciful. The suspicion must also be more than a vague feeling of unease. If someone thinks a transaction is suspicious, they are not expected to know the exact nature of the criminal offence or that particular funds were definitely those arising from the crime. They may have noticed something unusual or unexpected and, after making enquiries, the facts do not seem normal or make commercial sense. There does not have to be evidence that *money laundering, terrorist financing,* or *the financing of proliferation* is taking place for there to be a suspicion.

71. If someone has not yet formed a suspicion, but they have cause for concern, a *supervised person* may choose to ask the *customer* or other parties more questions. This decision will depend on what is already known, and how easy it is to make enquiries. The provisions under section 8.5 of *this Handbook* regarding tipping off may also need to be considered.

72. If there is a belief that a *customer* is innocent, but there are suspicions that another party to the *business relationship* or *one-off transaction* is engaged in *money laundering,* the *financing of terrorism*, or the *financing of proliferation* a *supervised person* may need to consider referring the *customer* for specialist advice regarding the risk that they may be a party to a criminal offence.

73. Section 6.4 of *this Handbook* and the sector-specific sections of *this Handbook* below provide several standard warning signs which may suggest an increased risk of *money laundering,* the *financing of terrorism,* or the *financing of proliferation* and therefore give cause for concern. However, whether someone has a suspicion is a matter of their own judgement.

9.2.3.3 **Reasonable grounds to suspect: the objective test of knowledge or suspicion**

74. Articles 30 and 31 of the *Proceeds of Crime Law*, when read with Article 29 of the *Proceeds of Crime Law* and Articles 15 and 16 of the *Terrorism Law* provide for an offence to be committed when dealing with, using, concealing etc criminal or terrorist property where there are reasonable grounds to know or suspect that property represents the proceeds of criminal conduct or instrumentalities, or terrorist property.

75. This means that a person would commit an offence even if they did not know or suspect that a *money laundering* or *terrorism financing* offence was being committed and is determined by whether a reasonable person would suspect that criminality had occurred. In other words:

- were there factual circumstances from which a reasonable person, engaged in a similar business, should have inferred knowledge, or formed the suspicion that another was engaged in *money laundering,* the *financing of terrorism.*
- was there knowledge of circumstances which would put a reasonable person on enquiry?

9.3 Procedures for reporting

76. Reporting procedures provide the interface between *CDD* measures carried out by a *supervised person* and the work of the *FIU's* intelligence wing. Like all *policies and procedures*, they should be:

- drafted in a way that can be easily understood by *Employees;*
- tailored to the *supervised person's BRA*; and
- applied in every case where functions are outsourced (in line with section 2.4.4 of *this Handbook*).

Statutory requirements (paraphrased wording)

77. *Article 21 of the Money Laundering Order requires that a relevant person must establish and maintain reporting procedures which:*

- *communicate to employees the identity of the MLRO (and any Deputy MLROs) to whom an internal SAR is to be made;*
- *provide for that report to be considered by the MLRO (or Deputy MLRO) in the light of all other relevant information for the purpose of determining whether or not the information or other matter contained in the report gives rise to knowledge, suspicion or reasonable grounds for knowledge or suspicion that another person is engaged in money laundering or the financing of terrorism;*
- *allow the MLRO (or Deputy MLRO) to have access to all other information which may be of assistance in considering the report;*
- *provide for the information or other matter contained in an internal SAR to be disclosed as soon as is practicable by the MLRO (or Deputy MLRO) to the FIU using the approved form, where the MLRO (or Deputy MLRO) knows, suspects or has reasonable grounds to know or suspect that another person is engaged in money laundering or the financing of terrorism; and*
- *provide for additional information relating to a report to be given by the MLRO (or Deputy MLRO) to the FIU.*

78. *Article 22 of the Money Laundering Order states that if a Deputy MLRO, on considering an internal SAR, concludes that it does not give rise to knowledge, suspicion or reasonable grounds for knowledge or suspicion that another person is engaged in money laundering or the financing of terrorism, the Deputy MLRO need not forward it to the MLRO. If a Deputy MLRO, on considering an internal SAR, has concluded that it does give rise to knowledge, suspicion or reasonable grounds for knowledge or suspicion that another person is engaged in money laundering or the financing of terrorism, although the SAR must still be forwarded to the MLRO, the MLRO need not consider that question. The effect of this is to require a report to be considered by the MLRO only in a case where the Deputy MLRO is not able to come to a conclusion.*

9.3.1 Internal *SARs*

AML/CFT/CPF Codes of Practice

[COP84] In addition to reporting procedures that must be maintained under Article 21 of the *Money Laundering Order*, a *supervised person* must maintain procedures that:

- highlight that reporting requirements extend to potential *business relationships* and *one-off transactions* that are declined (i.e., where no *business relationship* is established, or *one-off transaction* carried out);
- highlight that internal *SARs* are to be made regardless of the amount involved in a transaction or relationship and regardless of whether it is thought to involve tax matters;
- highlight the importance of making an internal *SAR* **as soon as practicable;**
- require internal *SARs* to be made in a set format and to include as full a statement as possible of:

i) the information or matter giving rise to knowledge, suspicion or reasonable grounds for knowledge or suspicion;

ii) the date that the information or matter came to the employee's attention;

iii) the date of submission of the internal SAR; and

iv) full details of the customer, transaction or activity that the supervised person holds on its records.

› require internal *SARs* to be acknowledged by the *MLRO* (or *Deputy MLRO*) **as soon as practicable;**

› require the *MLRO* (or *Deputy MLRO*) to record all internal *SARs* in a register which includes the following:

i) the date that the information or matter came to the Employee's attention;

ii) date of the internal SAR;

iii) identity of the individual making the internal SAR; and

iv) information to allow supporting documentation to be retrieved in a timely manner.

[COP85] A *supervised person* must not allow internal *SARs* to be filtered by line management such that they do not reach the *MLRO* (or *Deputy MLRO*). Where procedures allow *Employees* to discuss relationships and transactions with line managers before an internal *SAR* is made, those procedures must emphasise that the decision on reporting remains with the *Employee* and not the line manager.

[COP86] A *supervised person* must establish and maintain arrangements for disciplining any *Employee* who fails, without reasonable excuse, to make an internal *SAR* where they have knowledge, suspicion or reasonable grounds for knowledge or suspicion, or does not do so **as soon as practicable**.

Guidance notes

79. A *supervised person* may demonstrate that it has established and maintained arrangements for disciplining *Employees* by ensuring that employment contracts and employment *Handbook*s provide for the imposition of disciplinary sanctions for failing to report knowledge, suspicion or reasonable grounds for knowledge or suspicion without reasonable excuse or failing to report as soon as practicable.

80. A *supervised person* may demonstrate that *Employees* make internal *SARs* as soon as practicable where the *MLRO* (or *Deputy MLRO*) periodically considers (by business area if appropriate):

› the amount of time taken between information or a matter coming to an *Employee's* attention and the date of the internal *SAR* and concludes that it is reasonable;

› the number and content of internal *SARs* and concludes that both are consistent with the *supervised person's BRA*.

9.3.2 External *SARs*

Overview

81. The *MLRO* (or *Deputy MLRO*) must consider each internal *SAR*. The *Money Laundering Order* requires that the *MLRO* (or *Deputy MLRO*) has access to all necessary records. The *MLRO* (or *Deputy MLRO*) may also require further information to be obtained from the *customer*. Any such approach will need to be made sensitively and probably by someone other than the *MLRO* (or *Deputy MLRO*) to minimise the risk of alerting the *customer* that a report to the *FIU* may be under consideration (though this may not yet be tipping off).

82. When considering an internal *SAR* the *MLRO* (or *Deputy MLRO*), taking a risk-based approach, will need to strike an appropriate balance between the requirement to make a report to the *FIU* as soon as practicable, especially if consent is required, and any delay that might arise from searching a number of potentially unlinked systems and records that might hold relevant information.

83. For *supervised persons* who are subject to the requirements of the EU Legislation (Information Accompanying Transfers of Funds) (Jersey) Regulations 2017 (as amended to account for *MVTS supervised persons* and *VASP supervised persons* (as appropriate), and which are transacting with group counterparties in a different jurisdiction, those *supervised persons* are required to file a *SAR* in each jurisdiction to which the transaction relates.

AML/CFT/CPF Codes of Practice

[COP87] In addition to reporting procedures that must be maintained under Article 21 of the *Money Laundering Order*, a *supervised person* must maintain *procedures* that:

› require the *MLRO* (or *Deputy MLRO*) to document all enquiries made in relation to each internal *SAR*;

› require the *MLRO* (or *Deputy MLRO*) to document the basis for reporting to the *FIU* or deciding to not make such a report. This must be retained with the internal *SAR*;

› require the *MLRO* (or *Deputy MLRO*) to record all external *SARs* in a register which includes the following:

   i) date of the external SAR;

   ii) name of the individual making the external SAR and the capacity in which they are doing so (e.g., as the supervised person's MLRO or Deputy MLRO); and

   iii) information to allow supporting documentation to be retrieved in a timely manner.

› require the *MLRO* (or *Deputy MLRO*) to inform the *FIU* where relevant information is subsequently discovered.

Guidance notes

84. A *supervised person* may demonstrate that an internal *SAR* is considered in light of all other *supervised* information when the following are taken into account:

› the business and risk profile for the subject of the report;

› the complexity and duration of the *business relationship*;

› transaction patterns and volumes, and previous patterns of instructions;

- any connected accounts or relationships. Connections can be commercial e.g., linked transactions or common referrals, or through individuals e.g., third parties, *Beneficial owners and/or controllers* or account signatories; and
- the risk that assets will dissipate.

85. A *supervised person* may demonstrate that the *MLRO* (or *Deputy MLRO*) reports as soon as practicable where the board considers:

- the typical amount of time taken by the *MLRO* (or *Deputy MLRO*) to consider an internal *SAR* (being the time taken between the date of the internal *SAR* and the date of the external *SAR*/decision to not report) and concludes that it is reasonable; and
- the number of internal *SARs* not considered within a period of time judged by the board/senior management to be reasonable, together with an explanation.

Refer to section 2.1 *of this Handbook* for an explanation of the meaning of "the board" in the context of this paragraph.

9.4 *FIU* Consent

Overview

86. Protective reports **before** or **after** doing an act are not equal options which a *supervised person* can choose between.

- a report should be made **before doing an act** where a *customer* instruction is received prior to an activity or transaction taking place, or arrangements being put in place. However, when a transaction which gives rise to concern is already within an automated clearing or settlement system where a delay would lead to a breach of a contractual obligation or where it would breach market settlement or clearing rules, the *MLRO* (or *Deputy MLRO*) may need to let the transaction proceed and report it later.
- a report should be made **after doing an act** where something appears suspicious only with the benefit of hindsight or following the receipt of additional information.

87. Under Article 32(4) of the *Proceeds of Crime Law,* if a *SAR* was made **before doing an act,** a *supervised person's MLRO* (or *Deputy MLRO)* should request consent from the *FIU* for a specific transaction (for example, a distribution). Such consent requests should be sent to the *FIU* via the *SAR* portal (POLSAR), either as part of an initial *SAR* submission, or as part of a continuation report. Where no specific consent for an act is being sought under Article 32(4) of the *Proceeds of Crime Law*, the *FIU* will usually only issue an acknowledgement in response to a *SAR*. Further guidance on the consent regime is provided on the FIU's website and may be updated from time to time.

88. While waiting for the *FIU* to provide consent to proceed with a transaction or activity, if the *FIU* notifies a *supervised person* that consent will not be given, a *supervised person* should be aware of the risk of committing a tipping off offence where it fails to act on a *customer* instruction. In any written communication with that *customer* regarding the instruction, it should consider using generalised wording to explain the situation.

89. In a situation where consent is not given, a *supervised person* should contact the *FIU* for guidance on what information can be provided to the *customer* (though the *FIU* is not obligated to provide such guidance).

90. Where a *supervised person* does not wish to or decides not to act upon a *customer's* instruction, this may lead to civil proceedings being instituted by the *customer* for breach of contract. In these circumstances it may be necessary for the *supervised person* to seek legal advice or direction from the law courts.

91. A *supervised person* may reduce the risk of civil proceedings by ensuring that *customers'* terms of business specifically:

› allow an instruction to be delayed or deferred pending investigation;

› exclude breaches in circumstances where following a *customer* instruction may lead to the *supervised person* committing an offence.

9.5 Tipping off

Overview

92. In this section, reference to a "disclosure" is to the disclosure of matters **related** to a *SAR* or an investigation (and not the disclosure of suspicion or knowledge **through** a *SAR*).

93. Except as otherwise provided, where a person knows or suspects that an internal or external *SAR* has been or will be made, a person will commit a tipping off offence where they disclose to another person:

› the fact that they have made, or will make, an internal or external *SAR*; or

› any information relating to such a *SAR*.

94. Except as otherwise provided, where a person knows or suspects that the Attorney General or any police officer is acting or proposing to act in connection with a criminal investigation into *money laundering* or the *financing of terrorism* that is being or is about to be conducted, a person will commit a tipping off offence where they:

› disclose to another person any information relating to the investigation; or

› interfere with material which is likely to be relevant to such an investigation.

95. Among other things, the effect of this is that a *supervised person* or *employee* of a *supervised person*:

› cannot, **at the time**, tell a *customer* that a transaction or activity **is being delayed** because an internal *SAR* is about to be made or has been made to the *MLRO* (or *Deputy MLRO*);

› cannot, **at the time**, tell a *customer* that a transaction or activity **is being delayed** because an external *SAR* is about to be made or awaiting consent from the *FIU*;

› cannot **later** tell a *customer* that a transaction or activity **was delayed** because an internal or external *SAR* had been made;

› cannot tell the *customer* that law enforcement is conducting an investigation.

96. However, a tipping off offence is not committed when a *supervised person* discloses that an internal *SAR* has been made; that it will make or has made an external *SAR*; information relating to such *SARs*; or information relating to a criminal investigation, where the above information is disclosed to its:

› *Lawyer* –to obtain legal advice or for the purpose of legal proceedings; or

› *Accountant* – for the purpose of enabling the *Accountant* to provide certain services, e.g., in order to provide information that will be relevant to the statutory audit of a *supervised person's* financial statements;

except, where the disclosure is made with a view to furthering a criminal purpose.

97. Nor is a tipping off offence committed when a ***Lawyer*** discusses that disclosure with its *customer*, where this is in connection with the provision of legal advice or for the purpose of actual or contemplated legal proceedings (except where the discussion is with a view to furthering a criminal purpose). **However, no similar provision is made for an *Accountant* to discuss a disclosure with its *customer*.**

98. In addition, a tipping off offence will not be committed where a disclosure is permitted under the *Tipping Off Regulations* – known as a "**protected disclosure**". A disclosure will be a protected disclosure where it meets the conditions set in the *Tipping Off Regulations:*

› made as a result of a legal requirement;

› made with the permission of the *FIU*;

› made by an *Employee* of a person to another *Employee* of the same person;

› a disclosure within a *financial group* or network;

› made to another *supervised person* (but not an *equivalent business*); or

› made to the *JFSC*.

99. Except where it is made pursuant to a legal requirement or with the permission of the *FIU*, a disclosure will not be a protected disclosure under the *Tipping Off Regulations* unless it is made in good faith for the purpose of preventing or detecting *money laundering* or the *financing of terrorism*.

100. Whilst the *Tipping Off Regulations* permit disclosure **of the fact** that a *SAR* has been or will be made and/or any information relating to the *SAR*, they do not permit the *SAR* form or copy of the *SAR* form to be disclosed (except where done pursuant to a legal requirement or by one *employee* of a person to another *employee* of that person within Jersey).

101. In a case where a *supervised person*:

› is the *customer* of a *Financial Institution* or a *DNFBP* (A) that is not a *supervised person*; and

› is acting for one or more third parties; and

› has undertaken to make a disclosure to A when it makes a *SAR* in respect of any of those third parties;

a tipping off offence is committed, except where such a disclosure is made with the permission of the *FIU*.

102. Care should also be exercised where a person is also subject to legislation in force outside Jersey. Notwithstanding that a disclosure may be a protected disclosure under the *Tipping Off Regulations*, this protection will not extend to an offence that is committed where a disclosure is not permitted under that other legislation.

Statutory requirements (paraphrased wording)

103. *Article 35(4) of the Proceeds of Crime Law and Article 35(4) of the Terrorism Law make it an offence to disclose the fact that a SAR has been or will be made, or any information otherwise relating to such a SAR, if a person knows or suspects that a SAR has been or will be made, except if the disclosure is a protected disclosure under the Tipping Off Regulations.*

104. *Article 35(2) of the Proceeds of Crime Law and Article 35(2) of the Terrorism Law make it an offence to disclose any information relating to an investigation, or to interfere with material which is likely to be relevant to such an investigation, where a person knows or suspects that the Attorney General or any police officer is acting or proposing to act in connection with money laundering or financing of terrorism investigation - except if the disclosure is a protected disclosure under the Tipping Off Regulations.*

105. *Article 35(5) of the Proceeds of Crime Law and Article 35(5) of the Terrorism Law provide for the States of Jersey to make Regulations, specifying cases where a disclosure or interference shall not amount to an offence.*

106. *Articles 35(2) and (4) of the Proceeds of Crime Law do not apply to the disclosure of an investigation or SAR which is made by a relevant person to:*

- *a professional legal adviser in connection with the provision of legal advice or for the purpose of actual or contemplated legal proceedings; or*
- *an Accountant for the purpose of enabling that person to provide external accounting services, tax advice, audit services or insolvency services;*
- *so long as it is not made with a view to furthering a criminal purpose.*

107. *A person who is guilty of an offence under Article 35 of the Proceeds of Crime Law or the Terrorism Law is liable to imprisonment for a term not exceeding 5 years or a fine, or to both.*

108. *Regulation 2 of the Tipping Off Regulations lists disclosures that are protected disclosures. A disclosure will be protected where:*

- *it is made in good faith for the purpose of preventing or detecting money laundering or the financing of terrorism and it falls with any of the cases specified in Regulations 3 to 7 of the Tipping Off Regulations;*
- *it is made in good faith for the purpose of preventing or detecting money laundering or the financing of terrorism and it is made to a person's MLRO (or Deputy MLRO);*
- *it is required to be made by statute in Jersey or law elsewhere;*
- *it is made with the permission of the FIU.*

109. *A disclosure that is required to be made by statute or law may include transmission of the form used to make a SAR (or copy thereof).*

110. *Regulation 3 of the Tipping Off Regulations permits an employee of a relevant person (D) to make a disclosure to another employee of the same person (R). Such a disclosure may include transmission of the form used to make a SAR (or copy thereof) so long as the recipient of the disclosure is a person within Jersey. Such a disclosure may also include the name of the individual who has made the internal SAR.*

111. *Where a further disclosure is made by R in accordance with the Tipping Off Regulations (other than under Regulation 3), it may not disclose the identity of D.*

112. *Regulation 4 of the Tipping Off Regulations permits a relevant person and an Employee of such a person (D) to make a disclosure to a person in another part of its financial group or with whom D shares common ownership, management or compliance control (R). Such a disclosure may not include transmission of the form used to make a SAR (or copy thereof), nor may it disclose the identity of the individual who has made the internal SAR.*

113. *Where a further disclosure is made by R in accordance with the Tipping Off Regulations, it may not disclose the identity of D, where D is an individual.*

114. *Regulation 5 of the Tipping Off Regulations permits a relevant person and an Employee of such a person (D) to make a disclosure to another relevant person (R) where the disclosure relates to a person who is a customer (or former customer) of both D and R, or relates to a transaction, or provision of a service, including both D and R. Such a disclosure may not include transmission of the form used to make a SAR (or copy thereof), nor may it disclose the identity of the individual who has made the internal SAR.*

115. *Where a further disclosure is made by R in accordance with the Tipping Off Regulations, it may not disclose the identity of D nor D's MLRO (or Deputy MLRO).*

116. *Regulation 6 of the Tipping Off Regulations permits a relevant person and an Employee of a relevant person to make a disclosure to any of the following:*

- *a customs officer, a police officer or any employee of the FIU;*
- *the JFSC.*

117. *Where a further disclosure is made by any of the above in accordance with the Tipping Off Regulations (other than under its Regulation 6), it may not disclose the identity of the relevant person, except where the recipient is a customs officer, a police officer, any employee of the FIU, or the Commission.*

AML/CFT/CPF Codes of Practice

[COP88] In addition to reporting procedures that must be maintained under Article 21 of the *Money Laundering Order*, a *supervised person* must maintain procedures that remind *employees* making internal *SARs* of the risk of committing a tipping off offence.

9.5.1 *CDD* Measures

Overview

118. Article 13(1) of the *Money Laundering Order* requires identity to be found out and evidence of identity obtained **before** the establishment of a *business relationship* or **before** carrying out a *one-off transaction*, except in some limited circumstances. Article 13(1)(c) of the *Money Laundering Order* further requires that *identification measures* be applied where a *supervised person* suspects *money laundering* or the *financing of terrorism* (at any time) or has doubts about the veracity or adequacy of documents, data or information previously obtained under *CDD* measures during the course of a *business relationship*.

119. Where a *supervised person* suspects *money laundering* or the *financing of terrorism*, the application of *identification measures* could unintentionally lead to the *customer* being tipped off if the process is not managed with due care.

120. In circumstances where an external *SAR* has been made, and where there is a requirement to apply *identification measures*, the risk of tipping off a *customer* (and its advisers) may be reduced by:

- ensuring that *employees* applying *identification measures* are aware of tipping off provisions and are provided with adequate support, such as specific training or assistance;
- obtaining advice from the *FIU* where a *supervised person* is concerned that applying *identification measures* will lead to the *customer* being tipped off.

121. Where a *supervised person* reasonably believes that the application of *identification measures* could lead to the *customer* being tipped off, then under Article 14(6) of the *Money Laundering Order* it is not necessary to apply such measures, where an external *SAR* has been made, and the *FIU* has agreed that the measures need not be applied.

122. Making reasonable enquiries to a *customer* in a tactful manner regarding the background to a transaction or activity that is inconsistent with the *customer's* established profile is prudent practice and forms an integral part of *CDD* measures. Such enquiries, when conducted appropriately, are less likely to result in a tipping off offence being committed.

9.5.2 Terminating a business relationship

Overview

123. The giving of consent to proceed by the *FIU* following an external *SAR* submission is not intended to override normal commercial judgement, and a *supervised person* is not obligated to continue a *business relationship* with a *customer* they have reported upon if such action would pose a commercial risk.

124. A decision to terminate a *business relationship* is a commercial decision (except where there is a requirement to do so under Article 14 of the *Money Laundering Order*), and a *supervised person* is free to make such judgements. However, in certain circumstances a *supervised person* should consider liaising with the *FIU* to assess whether it is likely that termination would tip off the *customer* or affect an investigation in any way. If there is continuing suspicion and there are funds which need to be returned to the *customer*, a *supervised person* should seek advice from the *FIU*.

9.6 Disclosure to group companies and networks

Overview

125. Whilst the focus of the *Money Laundering Order* is on the role that a particular *supervised person* has in preventing and detecting *money laundering* or the *financing of terrorism*, where a *supervised person* is part of a group or larger network it is also important that they play their part in the prevention and detection of *money laundering* and the *financing of terrorism* at group or network level.

126. Accordingly, it is important that there should be no legal impediment to providing certain information to a group company or network.

127. Where a *supervised person* also wishes to disclose information to another *supervised person* (something that is anticipated under the *Tipping Off Regulations*), it will first be necessary to ensure that there is a proper basis for doing so, e.g., the conditions set out in the statutory requirements below are met.

Statutory requirements (paraphrased wording)

128. *Article 22A of the Money Laundering Order allows a relevant person to disclose the following to any person or institution with which the relevant person shares common ownership, management or compliance control, or (where different) any person within the same financial group, where such disclosure is appropriate for the purpose of preventing and detecting money laundering and the financing of terrorism:*

- *information contained in any report made to the MLRO (or Deputy MLRO);*
- *information provided to the FIU that is in addition to that contained in an external SAR;*
- *any other information that is kept under the Money Laundering Order.*

129. *Article 1(5) of the Money Laundering Order states that a person is a member of the same financial group as another person if there is, in relation to the group, a parent company or the legal person that exercises control over every member of that group for the purposes of applying group supervision under:*

- *the Core Principles for Effective Banking Supervision published by the Basel Committee;*
- *the Objectives and Principles of Securities Regulation issued by IOSCO; or*
- *the Insurance Supervisory Principles issued by IAIS.*

9.7 Investigation and the use of court orders

Overview

130. Following the receipt of a *SAR* and initial enquiries by the *FIU*, reports are allocated to financial investigation officers for further investigation. Intelligence from reports submitted to the *FIU* is then disseminated to other intelligence agencies, as appropriate.

131. Where additional information is required from a reporting institution following a *SAR*, it will generally be obtained pursuant to a **production order** issued by the Royal Court under the *Proceeds of Crime Law*, *Terrorism Law*, Investigation of Fraud (Jersey) Law 1991 and the Criminal Justice (International Co-operation) (Jersey) Law 2001, or a ***customer* monitoring order** under the *Terrorism Law*. It is a criminal offence to fail to comply with the terms of any order received under the above legislation.

132. During an investigation, a *supervised person* may be served with an order designed to restrain particular funds or property pending the outcome of an investigation. It should be noted that the restraint order may not apply to all funds or assets involved within a particular *business relationship* and a *supervised person* should consider what, if any, funds and assets may still be utilised subject to having obtained the appropriate consent from the *FIU*.

133. Upon the conviction of a defendant, a court may order the confiscation of their criminal proceeds or the confiscation of assets to a value representing the benefit of their criminal conduct, which may require the realisation of assets which were **legitimately obtained**. A *supervised person* may be served with a confiscation order in relation to **any funds or property** belonging to that defendant. For example, if a person is found to have benefited from drug dealing to a value of £100,000, then the court may order the confiscation of **any assets** belonging to that person to a value of £100,000. Confiscation of the proceeds of criminal conduct is becoming common place within many jurisdictions, and legislation in place in Jersey provides a mechanism by which overseas criminal confiscation orders may be recognised. Overseas civil confiscation orders may also be recognised in Jersey.

134. Property may also be forfeited in Jersey utilising civil proceedings under the *Terrorism Law.*

135. The *FIU* will, from time to time, issue liaison notices to all *supervised persons*, or to a particular category of business, with the goal of obtaining additional intelligence. The *FIU* will ensure that the requests contained within such notices are proportionate and reasonable in the circumstances. *Supervised persons* are requested to respond with any relevant information **as soon as reasonably practicable**.

9.7.1 Updates/Feedback from the FIU

Overview

136. Because a significant proportion of *SARs* received by the *FIU* relate to the accounts or transactions of non-Jersey residents and so are disseminated to overseas intelligence agencies, it may not be possible for the *FIU* to provide regular updates or feedback on individual disclosures. However, the *FIU* will provide statistics, trends, and advice on a regular basis to help enhance the quality of disclosures. Alternatively, a periodic newsletter may be issued. In addition, the States of Jersey Police Annual Report contains some information on disclosures, prosecutions, and confiscations.

9.8 Sanctions compliance reporting obligations under the *Sanctions and Asset-Freezing Law*

137. Jersey's financial sanctions reporting obligations are outlined on the Government of Jersey website, and more extensive sanctions guidance can be found on the *JFSC* website.

138. It is a criminal offence to contravene or to intentionally participate in activities knowing that the object or effect of them is to circumvent, to enable, or to facilitate the contravention of any of the prohibitions in respect of Jersey's financial sanctions regimes.

139. Jersey's financial sanctions regimes are rules-based and designed to prevent sanctions breaches. They can relate to all sorts of *financial crimes*, such as *money laundering*, the *financing of terrorism*, the *financing of proliferation*, bribery, corruption, misappropriation of funds, market abuse etc. Sanctions breaches can lead to a potential prosecution for criminal offences and/or financial penalties and cause reputational damage to the *supervised person* and to Jersey as an international financial centre.

140. Jersey implements both *UNSC* sanctions and autonomous *UK* sanctions by implementing the relevant *UK* Sanctions Regulations through the *Targeted Financial Sanctions Measures.*

141. The list of active sanctions regimes is available on the *JFSC* website and provides further explanation of the sanctions legal framework, including:

- targeted financial sanctions related to terrorism and *terrorist financing*
- targeted financial sanctions related to proliferation and *proliferation financing*
- other sanctions regimes in effect in Jersey

142. Sanctions compliance reporting obligations under the *Sanctions and Asset Freezing Law* are separate and distinct from any legal obligation to submit a *SAR*. For example, the *Sanctions and Asset Freezing* Law requires notification to *the Minister* concerning suspected financial sanctions breaches, *sanctioned persons,* and frozen assets. In some circumstances, it may be necessary to submit both reports, i.e., an external *SAR* to the *FIU* and a sanctions compliance report to the *FSIU*.

143. *The Minister* is the "Competent Authority" for sanctions in Jersey. All communication regarding sanctions breaches and licencing should be made using the approved forms. These forms provide details on what information is required.

144. Even though Jersey has an independent sanctions regime, some cross-border transactions may trigger certain extra-territorial effects and sanctions compliance reporting obligations in another jurisdiction. In Jersey, failure to comply with sanctions compliance reporting obligations is a criminal offence.

145. In this section, reference to a 'person' is a reference to a natural person, as well as a legal person, body or entity. *'Designated person'* is defined in the Glossary of *this Handbook*, and essentially means persons who are subject to financial sanctions. References to the 'listing' of a person means their inclusion on the lists of *designated persons*. Sanctions designations lists are available on the *JFSC* website.

Statutory requirements (paraphrased wording)

146. *Under Article 1 of the Sanctions and Asset Freezing Law, a "relevant financial institution" includes:*

- *all financial services businesses, as specified in* Schedule 2 *of the Proceeds of Crime Law;*
- *a person (not being an individual) that is incorporated or constituted under the law of Jersey and carries on such financial services business in any part of the world.*

147. *Under Article 32 of the Sanctions and Asset Freezing Law, a relevant financial institution must inform the Minister as soon as practicable if -*

- *(a) it holds an account of a person, has entered into dealings or an agreement with a person or has been approached by or on behalf of a person;*
- *(b) it knows, or has reasonable cause to suspect, that the person;*
  - *i. is a designated person; or*
  - *ii. has committed, is committing or intends to commit an offence under this Law; and*
- *(c) the information or other matter on which the knowledge or reasonable cause for suspicion based came to it in the course of carrying on its business.*

148. *The information given to the Minister must include:*

- *the information or other matter on which the relevant financial institution's knowledge or reasonable cause for suspicion is based;*
- *any information that the relevant financial institution holds about the person by which the person can be identified; and*
- *if the person is a customer or client of the institution, the nature and amount or quantity of any funds or economic resources held by the institution for the person at the time when the institution first had the knowledge or reasonable cause for suspicion.*

149. *The Minister retains the power to require additional information and to disclose information under certain conditions.*

150. *By exception, under Article 15 of the Sanctions and Asset Freezing Law, the relevant financial institution may credit frozen accounts in certain circumstances. This activity must be reported to the Minister, as soon as practicable, but in any case, within 14 days.*

151. *Under Article 35(1) of the Sanctions and Asset-Freezing Law, a person commits an offence, and is liable to imprisonment for a term of 12 months and to a fine of level 3 on the standard scale, if the person, without reasonable excuse, refuses or fails within the time and in the manner specified (or, if no time has been specified, within a reasonable time) to comply with sanctions reporting requirements.*

152. *Under Article 35(2) of the Sanctions and Asset Freezing Law, a person commits an offence, and is liable to imprisonment for a term of 2 years and to a fine, if the person: –*

- *(a) knowingly or recklessly gives any information, or produces any document, that is false in a material particular in response to a requirement of sanctions reporting obligations.*
- *(b) with intent to evade the reporting provisions, destroys, mutilates, defaces, conceals or removes a document; or*
- *otherwise intentionally obstructs the Minister in the exercise of the Minister's powers.*

Guidance notes

153. The most common types of financial sanctions include:

- targeted asset freezes, which are usually applied to named individuals, entities, and bodies, restricting their access to and ability to use funds and economic resources;
- restrictions on access to a wide variety of financial markets and services, applicable to named individuals, entities, and bodies, to specified groups or to entire sectors, such as investment bans, restrictions on access to capital markets, directions to cease banking relationships and activities, requirements to notify or seek authorisation before certain payments are made or received, and restrictions on provision of financial, insurance, brokering, advisory services or other financial assistance; and
- directions to cease all business of a specified type with a specific person, group, sector, territory, or country.

154. Financial sanctions legislation will contain prohibitions on carrying out certain activities or behaving in a certain way where financial sanctions apply. What is prohibited depends on the exact terms of the relevant financial sanctions regime.

155. A *relevant financial institution* should refer to the most up-to-date version of the sanctions legislation imposing the specific financial sanctions that apply in their case, to understand exactly what is prohibited and if there is a breach. We strongly encourage independent advice to be sought if there is any doubt in respect of this point.

156. If the financial sanction takes the form of an asset freeze, it is generally prohibited to:

- deal with the funds or economic resources belonging to or owned, held, or controlled by a *designated person*;
- make funds or economic resources available, directly or indirectly, to, or for the benefit of, a *designated person*; or
- engage in actions that directly or indirectly circumvent the financial sanctions.

157. The *relevant financial institution*, which knows or has a "reasonable cause to suspect" that it is in possession or control of, or is otherwise dealing with, the funds or economic resources of a *designated person*, may demonstrate their sanctions reporting compliance by undertaking and documenting the following:

- Immediately freeze funds or economic resources without notice and without delay;
- refrain from dealing with the funds or assets or making them available (directly or indirectly) to such persons unless licensed by *the Minister*;
- as soon as practicable, report any findings to the *FSIU*, together with any additional information that would facilitate compliance with the *Sanctions and Asset Freezing Law*;
- provide any further information concerning the frozen assets of *designated persons*, if required. Examples of information to be reported to *the Minister* may be found in Annex A to the *JFSC*'s Financial sanctions practical guidance.

158. "Reasonable cause to suspect" refers to an objective test that the Court uses to ascertain whether there were factual circumstances from which an honest and reasonable person should have inferred knowledge, or formed the suspicion, of a sanctions breach.

159. The requirement to disclose a breach to *the Minister* "as soon as practicable" after discovery of the breach is dependent on the circumstances in each case. Although it is reasonable for a person to take some time to assess the nature and extent of the breach, and/or seek advice, this should not delay an effective response to the breach. A *relevant financial institution* should demonstrate their decision-making process and document any reason for a reporting delay.

160. Where full disclosure is not possible, it is recommended that a *relevant financial institution* makes an early disclosure with partial information on the basis that it is still working out the facts and will make a further disclosure as soon as possible.

161. Sanctions reporting is not generally related to a tipping-off offence since sanctions designations are public. However, there may be circumstances when tipping off provisions may apply, such as when a *SAR* has been submitted for related suspected *money laundering*, or the *financing of terrorism,* or the *financing of proliferation*.

162. The sanctions landscape is constantly changing and evolving. It requires dedicated and qualified staff to ensure that all sanctions designation changes are reviewed and implemented without delay through effective sanctions screening and asset-freezing processes. A *relevant financial institution* may demonstrate an effective sanctions compliance culture by:

› having appropriate *policies and procedures* and *systems and controls* in place to ensure that there are dedicated staff assigned to sanction compliance monitoring and reporting;

› evidencing that relevant training is provided to the assigned employees and to management, including sanctions evasion techniques and identification of sanctions evasion;

› ensuring that the requisite report is filed in accordance with the legislation relevant to the particular sanctions regime and its guidance;

› appropriate sanctions reporting record-keeping.

The *JFSC* and the Government of Jersey provide regular updates on sanctions matters, and deliver sanctions webinars, workshops, and presentations. Further information, including a, description of sanctions regimes in effect in Jersey and their relevant guidance, is available on the *JFSC* website. Further sources of information in respect of *proliferation financing* risks and sanctions evasion typologies also available on the *JFSC's* Additional information sources – ML/TF/PF page.

10 SCREENING, AWARENESS AND TRAINING

10.1 Overview of section

1. An important control over the prevention and detection of *money laundering,* the *financing of terrorism and* the *financing of proliferation* is to ensure a supervised person can be confident that its *Employees*, *key persons* and *principal persons* are not criminals or associated with criminals.

2. Supervised persons must ensure those exercising significant influence and control are fit and proper persons and remain so; regular reference to a criminal record history is a way to evidence this.

3. Additionally, supervised persons need appropriately screened employees who are:

- alert to *money laundering*, *terrorist financing*, *and proliferation financing* risks; and
- well trained in the recognition of notable transactions or activity which may indicate *money laundering*, the *financing of terrorism*, or the *financing of proliferation* activity (see section 6 of *this Handbook*).

4. The effective application of even the best designed *systems and controls* (including *policies and procedures*) is compromised if *Employees* lack competence or integrity, or are unaware of, or fail to apply, *systems and controls* (including *policies and procedures*), or if *Employees* are not adequately trained.

5. It is essential that a *supervised person* takes action to make sure that *customer*-facing and other *Employees* are:

- competent and have integrity;
- aware of *policies and procedures* and their obligations under the *Anti-Money laundering and Counter-Terrorism Legislation* and the *AML/CFT/CPF Codes of Practice* issued under the *Supervisory Bodies Law;*
- trained in the recognition of notable transactions or activities (which may indicate *money laundering*, the *financing of terrorism*, or the *financing of proliferation*) or transactions and activity with *enhanced risk states* and/or *sanctioned persons.*

6. In particular, *customer*-facing Employees and those who handle, or are responsible for the handling of, *customers* and transactions will provide a *supervised person* with its strongest defence, or its weakest link.

7. As noted in the Glossary *of this Handbook*, for the purposes of *this Handbook* the term "*Employee*" should be understood to include officers of a *supervised person* and is not limited to individuals working under a contract of employment. It will include temporary and contract *Employees*, and the *Employee* of any external party fulfilling a function in relation to a *supervised person* under an outsourcing agreement or *Employee* of an *AMLSP* providing *AMLSP services* to the *supervised person* under an *AMLSP* agreement. For the purposes of this section, *employees* also include any agents acting as part of an *MVTS*' network, whereby an *MVTS* should treat employees of any agents as their own.

8. A *supervised person* should also encourage its *Employees* to maintain an active awareness of the risks of *money laundering,* the *financing*

10.2 *Screening of Employees*

Statutory requirements (paraphrased wording)

9. *Article 11(1)(d) of the Money Laundering Order requires a relevant person to maintain appropriate and consistent policies and procedures relating to screening of employees.*

AML/CFT/CPF Codes of Practice

[COP89] A *supervised person* must screen the competence and probity of the following *Employees* at the time of recruitment and where there is a subsequent change in an *Employee's* role:

- *customer*-facing *Employees* and other *Employees* handling, or being responsible for the handling of, *business relationships* or *one-off transactions*;
- *Employees* directly supporting *customer*-facing *Employees* or other *Employees* handling or responsible for the handling of *business relationships* or *one-off transactions*, e.g., individuals processing and book-keeping *customer* transactions;
- the *MLRO* (and any *Deputy MLRO*) and *MLCO*; and
- the board and senior management.

Guidance notes

10. With reference to the *AML/CFT/CPF Codes of Practice* at paragraph 8 above, a *supervised person* may demonstrate that an *Employee* is screened where it does one or more of the following, as appropriate for the nature of the *Employee's* role and responsibilities:

- obtains and confirms references provided;
- obtains and confirms employment history and qualifications disclosed;
- obtains details of any regulatory action taken against the individual (or absence of such action);
- obtains and confirms details of any criminal convictions (or absence of such convictions).

11. Enquiries into an individual's criminal past are required to be subject to the Rehabilitation of Offenders (Jersey) Law 2001, which prevents a *supervised person* requesting information from its directors, senior managers and other *Employees* (and prospective directors, senior managers and other *Employees*) about *convictions that are "spent",* except where provided for by the Rehabilitation of Offenders (Exceptions) (Jersey) Regulations 2002.

10.3 Obligations to promote awareness and to train

Overview

12. The *Money Laundering Order* requirements concerning both the promotion of awareness and the provision of training apply to *Employees* whose duties relate to the provision of a *supervised business* (defined in the Glossary *of this Handbook* as "*relevant employees*"). They do not apply to all *Employees* of a *supervised person*. However, *money laundering,* the *financing of terrorism, or* the *financing of proliferation* offences established in the *Proceeds of Crime Law, Terrorism Law* and other legislation are wider in scope, therefore all *Employees* will need to have a basic understanding of *money laundering,* the *financing of terrorism,* or the *financing of proliferation* and how they may manifest themselves. All *Employees* must also know and apply internal reporting procedures and know the identity of the *MLRO* (and, if applicable, the *Deputy MLRO*) and know how to contact them.

13. *Relevant employees* will include, among others, relationship managers, accounting and book-keeping staff, and stockbrokers.

Statutory requirements (paraphrased wording)

14. *Articles 11(9), (10), (10A), (11) and (12) of the Money Laundering Order require that a relevant person must, in relation to employees whose duties relate to the provision of a financial services business:*

- *take appropriate measures from time to time for the purposes of making them aware of:*
  - *the CDD, record-keeping, reporting and other policies and procedures for the purposes of preventing and detecting money laundering and the financing of terrorism;*
  - *the enactments in Jersey relating to money laundering and the financing of terrorism and any relevant Code of Practice.*
- *provide those employees from time-to-time with training in the recognition and handling of:*
  - *transactions carried out by or on behalf of any person who is or appears to be engaged in money laundering or the financing of terrorism;*
  - *other conduct that indicates that a person is or appears to be engaged in money laundering or the financing of terrorism.*

  Such training to include the provision of information on current money laundering techniques, methods and trends and on the financing of terrorism;
- *establish and maintain procedures that monitor and test the effectiveness of the relevant person's policies and procedures, employees' awareness and the training provided to employees, such testing having regard to the risk of money laundering that exist in respect of the relevant person's business and matters that may have an impact on that risk (e.g. size, nature and structure).*

AML/CFT/CPF Codes of Practice

[COP90] A supervised person must:

- provide Employees who are not relevant employees with a written explanation of the supervised person's and employees' obligations and potential criminal liability under the Anti-Money laundering and Counter-Terrorism Legislation, including the implications of failing to make an internal SAR;
- require such Employees to acknowledge that they understand the supervised person's written explanation and its procedures for making internal SARs.

[COP91] In the case of a supervised person who is a sole trader, that person must be aware of the enactments in Jersey relating to money laundering, the financing of terrorism, or the financing of proliferation and the AML/CFT/CPF Codes of Practice.

[COP92] In the case of a supervised person who is a sole trader, that person must be able to recognise and be aware of their obligations surrounding:

- transactions carried out by, or on behalf of, a person who is, or appears to be, engaged in money laundering, the financing of terrorism, or the financing of proliferation;
- other conduct that indicates a person is, or appears to be, engaged in money laundering, the financing of terrorism, or the financing of proliferation.

Guidance notes

15. A *supervised person* may demonstrate that it has satisfied awareness raising and training obligations that apply to *relevant employees* where it includes:

- *customer*-facing *Employees* and other *Employees* handling, or being responsible for the handling of, *business relationships* or *one-off transactions*;
- *Employees* directly supporting *customer*-facing *Employees* or other *Employees* handling, or being responsible for the handling of, *business relationships* or *one-off transactions*, e.g., individuals processing, book-keeping and accounting for *customer* transactions
- the *MLRO* (and any *Deputy MLRO*) and *MLCO*;
- the board and senior management.

16. A *supervised person* who is a *sole trader* may demonstrate that they are aware of relevant enactments and are able to recognise and are aware of their obligations surrounding transactions and other conduct (under paragraph COP90 above) where they have received formal training or through self-study.

10.4 Awareness of *relevant employees*

Overview

17. With the passage of time between training initiatives, the level of *Employee* awareness of the risk of *money laundering,* the *financing of terrorism,* or the *financing of proliferation* decreases. The utilisation of techniques to maintain a high level of awareness can greatly enhance the effectiveness of a *supervised person's* defences against *money laundering, financing of terrorism, or financing of proliferation* risk.

Guidance notes

18. A *supervised person* may demonstrate that it has appropriate awareness measures in place to make *relevant employees* aware of *policies and procedures* where it:

- provides them with a written explanation of its *BRA*, in order to provide context for those *policies and procedures*;
- provides them with case studies illustrating how products or services provided by the *supervised person* may be abused, in order to provide context for the application of *policies and procedures*;
- provides ready access to its *policies and procedures*.

19. A *supervised person* may demonstrate that it takes appropriate measures to make *relevant employees* aware of enactments in Jersey relating to *money laundering,* the *financing of terrorism,* or the *financing of proliferation* where it:

- provides *relevant employees* with a written explanation of the *supervised person's* and *Employee's* obligations and potential criminal liability under the *Proceeds of Crime Law, Terrorism Law, Directions Law, and the Targeted Financial Sanctions Measures,* including the implications of failing to make an internal *SAR*;
- provides *relevant employees* with a written explanation of the disciplinary measures that may be applied for failing to report knowledge, suspicion, or reasonable grounds for knowledge or suspicion, without reasonable excuse, or as soon as practicable;

› requires such *employees* to acknowledge that they understand the *supervised person's* written explanations and procedures for making internal *SARs*;

› reminds *Employees* of their obligations from time-to-time and the need to remain vigilant;

› circulates relevant material, e.g., material that is published by the *JFSC* or *FIU*, *FATF*, or *EU*, in order to provide context for enactments in Jersey;

› circulates relevant media reports, to provide context for enactments in Jersey.

20. A *supervised person* may demonstrate that it takes appropriate measures to make *relevant employees* who are officers (e.g., directors and equivalent) aware of enactments in Jersey relating to *money laundering,* the *financing of terrorism,* or the *financing of proliferation*, where the *supervised person* also explains how officers may be held personally liable for an offence committed by the *supervised person*.

10.4.1 Monitoring and testing effectiveness

Guidance notes

21. A *supervised person* may demonstrate that it maintains procedures for monitoring and testing the effectiveness of awareness-raising where it periodically tests *Employees'* awareness of:

› risks and *policies and procedures*; and

› statutory obligations;

and takes appropriate action where awareness is insufficient.

22. An *MVTS supervised person* may demonstrate the provision of training to or by agents as part of that *MVTS*'s network by conducting audits of the training delivered and being provided with assurances by that agent that any training delivered within the relevant period is appropriate and in conjunction with the requirements of *this Handbook*.

10.4.2 Technological developments

AML/CFT/CPF Codes of Practice

[COP93] Where a *supervised person* has identified a risk that may arise in relation to new products, services, business practices or technology, including where developed at group level or by outside developers (in Jersey and elsewhere), a *supervised person* must take steps to ensure that those involved in their development have a basic awareness of *money laundering,* the *financing of terrorism,* or the *financing of proliferation,* and of current *money laundering* techniques, methods and trends.

Guidance notes

23. A *supervised person* may demonstrate that developers have a basic awareness *of money laundering,* the *financing of terrorism,* or the *financing of proliferation,* and of current techniques, methods and trends where it:

› provides them with a written explanation of its *BRA*, in order to provide context for development work;

› provides case studies illustrating how new products, services, business practices and technology may be abused;

› circulates any relevant material, e.g., material that is published by the *JFSC* or *FIU*, the *FATF*, or the *EU*; and

- circulates relevant media reports.

24. A *supervised person* may also demonstrate that developers have a basic awareness of *money laundering,* the *financing of terrorism,* or the *financing of proliferation* and of current techniques, methods and trends, where it obtains assurances that similar measures to those set out in paragraph 33 are taken by group or outside developers.

10.5 Training of *Employees*

Overview

25. The guiding principle for all *AML/CFT/CPF* training should be to encourage *Employees*, irrespective of their level of seniority, to understand and accept their responsibility to contribute to the protection of the *supervised person* against the threat of *money laundering,* the *financing of terrorism,* or the *financing of proliferation*.

26. There can be a risk that more junior *Employees*, non-*customer* facing *Employees* and support *Employees* consider that their role is less crucial than, or secondary to, that of more senior or *customer*-facing colleagues. This can lead to failures to report important information because of assumptions that the information will have already been identified and dealt with by other colleagues. A *supervised person* should be aware of this risk and take steps to address it through the training provided.

AML/CFT/CPF Codes of Practice

[COP94] A *supervised person* must provide *Employees* with adequate training at appropriate frequencies. Such training must:

- be tailored to the supervised person and be relevant to the Employees to whom it is delivered;
- highlight to Employees the importance of the contribution that they can individually make to the prevention and detection of money laundering, the countering of terrorist financing, and the countering of proliferation financing;
- cover key aspects of legislation to prevent and detect money laundering, to counter terrorist financing, and to counter proliferation financing.

10.5.1 All relevant employees

Guidance notes

27. A *supervised person* may demonstrate the provision of adequate training to *relevant employees* where it addresses:

- the *supervised person* and *employees'* obligations under the *Proceeds of Crime Law, Terrorism Law, Directions Law, the Targeted Financial Sanctions Measures, Money Laundering Order* and *AML/CFT/CPF Codes of Practice* issued under the *Supervisory Bodies Law;*
- vulnerabilities of products and services offered by the *supervised person* (based on the *supervised person*'s *BRA*), and subsequent *money laundering*, *terrorist financing*, or *proliferation financing* risk;
- *policies and procedures*, and *Employees'* responsibilities under the same;
- application of risk-based *CDD policies and procedures*;

› recognition and examination of notable transactions and activity, such as activity outside of expected patterns, unusual settlements, abnormal payment or delivery instructions and changes in the patterns of *business relationships*;

› *money laundering, financing of terrorism*, or *proliferation financing* developments, including techniques, methods, trends and typologies (having regard for reports published by relevant Jersey authorities, *FATF* and *FSRBs)*;

› management of *business relationships* or *one-off transactions* subject to an internal *SAR*, e.g., risk of committing the offence of tipping off, and dealing with questions from such *customer*s, and/or their advisers.

10.5.2 The board or equivalents

Guidance notes

28. A *supervised person* may demonstrate the provision of adequate training to board members where (in addition to training for *relevant employees*) it addresses:

› conducting and recording a *BRA*;

› establishing a formal strategy to counter *money laundering*, the *financing of terrorism*, or the *financing of proliferation*; and

› assessing the effectiveness of, and compliance with, *systems and controls* (including *policies and procedures*).

10.5.3 The *MLCO*

Guidance notes

29. A *supervised person* may demonstrate the provision of adequate training to the *MLCO* where, in addition to training for *relevant employee*s, it addresses the monitoring and testing of compliance with *systems and controls* (including *policies and procedures*) in place to counter *money laundering*, the *financing of terrorism*, or the *financing of proliferation.*

10.5.4 The MLRO and Deputy MLRO(s)

Guidance notes

30. A *supervised person* may demonstrate the provision of adequate training to the *MLRO* (and, if applicable, *Deputy MLROs*) where, in addition to training for *relevant employees*, it addresses:

› the handling and validation of internal *SARs*;

› liaising with the *JFSC*, *FIU* and law enforcement;

› management of the risk of tipping off; and

› the handling of production and restraint orders.

10.5.5 Non-relevant employees

Guidance notes

31. A *supervised person* may demonstrate the provision of adequate training to *Employees* who are not *relevant employees* where it addresses:

› the threat of *money laundering*, the *financing of terrorism,* or the *financing of proliferation*; and

› procedures for making internal *SARs*.

10.5.6 Timing and frequency of training

Guidance notes

32. A *supervised person* may demonstrate the provision of training at appropriate frequencies by:

› providing all *Employees* with induction training **within 10 working days** of the commencement of employment and, when necessary, where there is a subsequent change in an *employee's* role; and

› delivering training to all *Employees* at least once every two years, and otherwise determining the frequency of training for *relevant employees* based on risk, with more frequent training delivered where appropriate.

10.5.7 Monitoring the effectiveness of screening, awareness, and training

Overview

33. Monitoring and testing the effectiveness of *policies and procedures*, awareness-raising measures and of training provided is a function of the *MLCO*, further detail of which is set out at Section 2.6 of *this Handbook*.

34. Such monitoring and testing should also be considered in the context of the board's periodic check that *systems and controls* (including *policies and procedures*) are operating effectively, as set out at section 2.4.1 of *this Handbook*.

10.6 Screening of key persons and principal persons

Overview

35. Where a key person or a principal person is also an *Employee* of the supervised person, the screening of that person will be in terms of this section. The attention of supervised persons is drawn to paragraph 11 above.

36. The Supervisory Bodies Law sets the expectation that key persons and principal persons be, at all times, fit and proper persons due to their heightened responsibilities and obligations.

37. A supervised person must regularly consider whether the criminal background of a key person or principal person is inconsistent with them being fit and proper to hold a key person or principal person roles.

38. Key persons and principal persons must be transparent when declaring their criminal history.

39. If there is a conflict between Section 10.6, and other parts of Section 10, the instructions and guidance in section 10.6 will prevail in situations concerning key persons and principal persons.

40. All references in this section to criminal record certificates mean a DBS check (or foreign equivalent).

Statutory requirements (paraphrased wording)

41. *Article 8(1) of the Supervisory Bodies Law gives the JFSC broad powers to carry out its supervisory duties. These include conducting examinations and requiring information from supervised persons.*

42. *Article 14(3) of the Supervisory Bodies Law permits the JFSC to refuse registration where an Applicant, Principal Person(s) or Key Person(s) are not fit and proper persons.*

43. *Article 14(4) of the Supervisory Bodies Law states that a person is not a fit and proper person, if they have been convicted of offences related to: money laundering; terrorist financing; proliferation financing; fraud; dishonesty; financial services laws; or are otherwise deemed unsuitable due to money laundering or terrorist financing risks.*

44. *Article 18(1)(d) of the Supervisory Bodies Law allows the JFSC to revoke the supervised person's registration if the applicant, principal persons or key persons of a supervised person are not fit and proper persons.*

45. *Article 34(2) of the Supervisory Bodies Law requires a registered person to promptly notify their supervisory body of any changes to key or principal persons, including if they cease their role or are convicted of relevant offences—unless the key person was appointed by an anti-money laundering services provider.*

AML/CFT/CPF Codes of Practice

[COP95] A supervised person must take reasonable steps to ensure that persons holding key persons and principal persons roles are at all times fit and proper in accordance with the applicable legislation and policies.

[COP96] Supervised persons must obtain a basic DBS check (or foreign equivalent) for key persons and principal persons for:

- new or additional principal person / key person roles;
- existing principal persons / key persons whenever there is a change of control;
- on an ongoing basis using a risk-based approach to ensure that these individuals continue to be fit and proper to hold these positions.

[COP97] Supervised persons must be able to provide the JFSC, upon request, documents supporting their assessment of the fitness and propriety of the key or principal person. This must include criminal record certificates, a summary of the checks conducted, and any relevant findings.

- Where an individual has not previously been authorised by the JFSC as a *principal or key persons* before 31 May 2026, the *supervised person* should obtain a criminal record certificate for:
  - i) the individual's current jurisdiction of residence; and
  - ii) each jurisdiction in which the individual has lived or worked for six months or more within the 10 years prior to the application.
- The criminal record certificate should be dated within six months of the date the application is submitted.

[COP98] A supervised person must notify the JFSC if there is any material change in relation to its key persons or principal persons that may impact their fitness and propriety.

Guidance notes

Generally

46. A supervised person may demonstrate that it has obtained a basic DBS check (or foreign equivalent) for key and principal persons on an ongoing basis by undertaking:

i) Periodic checks and renewals of criminal records at intervals using a risk-based approach. A supervised person can consider the frequency that is proportionate to the individual's risk profile, the nature of their role, and the size and complexity of the entity.

ii) This approach may result in more or less frequent criminal records checks for the key persons and principal persons depending on the level of risk associated with their roles or entities; risk profile of the jurisdiction or sector; and any history of non-compliance.

47. A supervised person may demonstrate that its key persons and principal persons remain fit and proper persons and suitable to hold their respective roles by regularly and proactively requiring the key and principal persons to confirm whether there has been any change in any relevant circumstances, concerning their criminal records history.

Definition of Principal Persons

48. For the purposes of criminal record certificates checks, principal persons shall be defined in terms of the Supervisory Bodies Law. For clarity:

i) Criminal records certificates will not be required for: passive investors of fund structures; limited partners for limited partnerships; unit holders for unit trusts; or vested beneficiaries, the settlor, objects of a power for trusts.

ii) Where the partnership is a legal person (Separate Liability Partnerships (SLPs), Incorporated Liability Partnerships (ILPs) or Limited Liability Partnerships (LLPs)), criminal records checks are required for beneficial owners with a holding of 10% or greater.

Previously Authorised Individuals

49. For individuals who were authorised as a *key or principal persons* before 31 May 2026:

i) On the first application submitted after 31 May 2026, the Supervised Person should obtain criminal record certificates covering all jurisdictions where the individual has lived or worked from the 31st of May 2026 to the date of the application.

ii) For any subsequent applications for new or different principal or key person roles, the supervised person should check whether the most recent criminal record certificate is dated within the last 12 months.

iii) If the certificate is dated within 12 months, a new one is not required. However, the individual must still:

- notify the JFSC of any change in role through the usual channels.

50. **New Certificate** If the most recent criminal record certificate is more than 12 months old at the time of a new application, the supervised persons should obtain a new criminal record certificates for:

- the current jurisdiction of residence; and
- each jurisdiction where the individual has lived or worked for six months or more since the date of the previous certificate.

51. The new certificate should be dated within six months of the application date.

52. In exceptional circumstances where a criminal record certificate cannot be obtained within the six-month period, and if doing so would unnecessarily interrupt the normal conduct of business or time to market is critical, the supervised person should:

- Document the reasons why a current certificate was not obtained or available.
- Obtain a certificate as soon as reasonably practicable thereafter.

53. Pending receipt of the refreshed certificate, the supervised person should take appropriate interim steps to satisfy itself that the individual is fit and proper.

11 RECORD-KEEPING

11.1 Overview of section

52. This section outlines the *statutory provisions* concerning record-keeping for the purposes of countering *money laundering*, the *financing of terrorism* or *proliferation financing*. It also sets *AML/CFT/CPF Codes of Practice* and provides *Guidance notes* on the keeping of records. More general obligations on *supervised persons* to maintain records in relation to their business are not addressed in this section – these may extend the period for which records must be kept.

53. Record-keeping is essential to facilitate effective investigation, prosecution, and confiscation of criminal property. If law enforcement agencies, either in Jersey or elsewhere, are unable to trace criminal property due to inadequate record-keeping, then prosecution for *money laundering,* the *financing of terrorism,* or the *financing of proliferation* and confiscation of criminal property may not be possible. Likewise, if the funds used to finance terrorist activity or proliferation activity cannot be traced back through the financial system, then the sources and the destination of *terrorist financing* or *proliferation financing* will not be identified.

54. Record-keeping is also essential to facilitate effective supervision, allowing the *JFSC* to supervise compliance by *supervised persons* with statutory requirements and *AML/CFT/CPF Codes of Practice*. Records provide evidence of the work that a *supervised person* has undertaken to comply with these requirements. Records also provide a necessary context for the opinion that may be prepared on the truth and fairness of a *supervised person's* financial statements by its external auditor.

55. Records may be kept:

- by way of original documents;
- by way of copies of original documents (certified where appropriate);
- in scanned form; or
- in computerised or electronic form.

11.2 Recording evidence of identity and other *CDD* measures

Overview

56. In relation to evidence of a *customer's* identity, a *supervised person* is required to keep a copy of, or references to, the evidence of the *customer's* identity obtained during the application of *CDD* measures.

57. In addition, a *supervised person* is required to keep supporting documents, data, and information in respect of a *business relationship* or *one-off transaction*. This consists of:

- accounts files;
- business correspondence records; and
- the results of any analysis undertaken regarding the *business relationship* or any transaction.

Statutory requirements (paraphrased wording)

58. *For the purpose of the record retention requirements set out below, Article A19 of the Money Laundering Order defines a 'relevant person' as including a person who was formerly a relevant person.*

59. *Article 19(2)(a) of the Money Laundering Order requires a relevant person to keep the following records:*

- *copies of evidence of identity or information that enables a copy of such evidence to be obtained;*
- *all the supporting documents, data, and information in respect of a business relationship or one-off transaction which is the subject of CDD measures, including the results of analysis undertaken in relation to the business relationship or any transaction.*

60. *Article 19(4) of the Money Laundering Order requires a relevant person to keep records in such a manner that they can be made available swiftly to the JFSC, police officer or customs officer for the purpose of complying with a requirement under any enactment, e.g. a production order under Article 40 of the Proceeds of Crime Law.*

61. *Articles 20(1) and 20(2) of the Money Laundering Order require a relevant person to keep records for at least five years from:*

iii) the end of the business relationship with the customer; or

iv) the completion of the one-off transaction.

62. *Article 20(5) of the Money Laundering Order allows the JFSC to require a relevant person to keep records for a period longer than five years.*

AML/CFT/CPF Codes of Practice

[COP99] As part of the supporting documents, data, and information to be kept in respect of a *business relationship* or one-off transaction, a *supervised person* must keep the following documents:

- accounts files; and
- business correspondence.

Guidance notes

63. Examples of business correspondence may include, but are not limited to:

- e-mails;
- letters;
- faxes;
- notes of telephone conversations.

64. A *supervised person* should consider, on a case-by-case basis, whether any records additional to those required under the *Money Laundering Order* or the *AML/CFT/CPF Codes of Practice* set out above should be kept for a particular *business relationship* or *one-off transaction*.

11.3 Recording transactions

Overview

65. Details of all transactions carried out by *a supervised person* with or for a *customer* in the course of carrying on a *supervised business* must be recorded. Additional records in support of such transactions, in whatever form they are used, e.g., credit/debit slips, cheques, will also be kept.

Statutory requirements (paraphrased wording)

66. *Article 19(2)(b) of the Money Laundering Order requires a relevant person to keep a record containing details of every transaction carried out with or for the customer in the course of a financial services business. In every case, sufficient information must be recorded to enable the reconstruction of individual transactions.*

67. *Article 19(4) of the Money Laundering Order requires a relevant person to keep records in such a manner that they can be made available swiftly to the JFSC, police officer or customs officer for the purpose of complying with a requirement under any enactment, e.g., a production order under Article 40 of the Proceeds of Crime Law.*

68. *Article 20(3) of the Money Laundering Order requires a relevant person to keep records relating to transactions for at least five years from the date when all activities relating to the transaction are completed.*

69. *Article 20(5) of the Money Laundering Order allows the JFSC to require a relevant person to keep records of transactions for a period that is longer than five years.*

AML/CFT/CPF Codes of Practice

[COP100] A record must be kept of the following for every transaction carried out in the course of a *business relationship or one-off transaction:*

- the name and address of the customer;
- if a monetary transaction, the kind of currency and the amount;
- if the transaction involves a customer's account, the number, name or other identifier for the account;
- the date of the transaction;
- details of the counterparty, including account details;
- the nature of the transaction; and
- details of the transaction.

[COP101] *Customer* transaction records must provide a clear and complete transaction history of incoming and outgoing funds or assets.

Guidance notes

70. A *supervised person* may demonstrate that it has kept details of a transaction where it records:

- valuation(s) and price(s);
- the form in which funds are transferred (e.g. cash, cheque, electronic transfer);
- memoranda of instruction(s) and authority(ies);

- memoranda of purchase and sale;
- custody of title documentation.

71. A *supervised person* may demonstrate that it has a clear and complete transaction history where it records **all transactions undertaken on behalf of a *customer*** within that *customer's* records. For example, a *customer's* records should include all requests for wire transfer transactions where settlement is provided other than from funds drawn from a *customer's* account with the *supervised person*.

72. When original vouchers or documents are used for account entry, e.g., credit/debit slips and cheques, and not returned to the *customer*, a *supervised person* may demonstrate that it has kept details of a transaction where such vouchers or documents are kept for at least one year to assist forensic analysis.

11.4 Other recording-keeping requirements

11.4.1 Corporate governance

AML/CFT/CPF Codes of Practice

[COP102] A *supervised person* must keep each *BRA* that it conducts and records under section 2.3 of *this Handbook* for a period of five years after the end of the calendar year in which it is superseded.

[COP103] A *supervised person* must keep adequate and orderly records of its *systems and controls* (including *policies and procedures*) that it must document under section 2.3 of *this Handbook* for a period of at least five years after the end of the calendar year in which they are superseded.

[COP104] A *supervised person* must keep adequate and orderly records showing how the Board/senior management has assessed both the effectiveness of, and compliance with, *systems and controls* (including *policies and procedures*) in line with section 2.3 of *this Handbook*, including reports presented by the *MLCO* on compliance matters and the *MLRO* on reporting, for a period of five years after the end of the calendar year in which a matter is considered.

[COP105] A *supervised person* must keep a record of what barriers (including cultural barriers) exist to prevent the operation of effective *systems and controls* (including *policies and procedures*) in line with section 4 2.4 of *this Handbook* for a period of five years after the end of the calendar year in which a matter is considered.

[COP106] A *supervised person* must keep adequate and orderly records to demonstrate the *MLRO* (and *Deputy MLRO*) and *MLCO's* experience and skills, independence, access to resources and technical awareness, in line with sections 2.6 and 2.7 of *this Handbook* for a period of five years after the end of the calendar year in which an individual ceases to act in said positions.

[COP107] A *supervised person* must keep adequate and orderly records to demonstrate that in line with section 2.4 of *this Handbook*:

- measures that are at least equivalent to AML/CFT/CPF Codes of Practice are applied by a *supervised person* through overseas branches; and

- subsidiaries are required to apply measures that are at least equivalent to AML/CFT/CPF Codes of Practice;
- for a period of five years after the end of the calendar year in which a measure is applied.

11.4.2 Identification measures

AML/CFT/CPF Codes of Practice

[COP108] Where a *supervised person* is required to apply an *identification measure* through an *AML/CFT/CPF Codes of Practice* set in sections 4, 5 and 7 of *this Handbook*, an adequate and orderly record of that measure must be kept in line with the record-keeping requirements set out in Part 4 of the *Money Laundering Order*.

[COP109] A *supervised person* must keep its risk assessment for each *customer* that has still to be remediated in line with section 4.9.2 of *this Handbook* for a period of five years after the end of the calendar year in which it is superseded.

11.4.3 Ongoing monitoring

Guidance notes

73. A *supervised person* may demonstrate that it has kept details of the results of analysis undertaken regarding a *business relationship* or any transaction where it keeps adequate and orderly records containing the findings of its examination of notable transactions and activity, i.e., those that:

- are inconsistent with the *supervised person's* knowledge of the *customer*;
- are complex or unusually large;
- form part of an unusual pattern; or
- present a higher risk of *money laundering,* the *financing of terrorism,* or the *financing of proliferation*;

for a period of five years from the end of the calendar year in which the examination is undertaken.

74. A *supervised person* may demonstrate that it has kept details of the results of analysis undertaken regarding a *business relationship* or any transaction where it keeps adequate and orderly records containing the findings of its examination of transactions and activity with a person which has a *relevant connection* to an *enhanced risk state*, for a period of five years from the end of the calendar year in which the examination is undertaken.

11.4.4 SARs

AML/CFT/CPF Codes of Practice

[COP110] A *supervised person* must keep registers of internal and external *SAR*s, maintained in line with procedures required under sections 9.3.1 and 9.3.2 of *this Handbook*.

[COP111] In line with procedures required under sections 9.3.1 and 9.3.2 of *this Handbook*, a *supervised person* must keep adequate and orderly records containing:

- a copy of the form and supporting documentation used to make any internal SAR for that customer;
- enquiries made in relation to that internal SAR and the decision of the MLRO (or Deputy MLRO) to make or not make an external SAR;
- where an external SAR has been made, a copy of the form used to make the external SAR and supporting documentation provided to the FIU; and
- relevant information passed to the FIU after making the external SAR;

for a period of five years from the date that a business relationship ends, or if in relation to a one-off transaction, for five years from the date that a transaction was completed.

Guidance notes

75. Depending on the volume of external *SARs* submitted, complexity of the *supervised person* and/or complexity of the matter subject to an external *SAR,* it may be decided to record continuation reports in a separate register to the initial external *SAR.* Where this is done, the *supervised person* should ensure that each continuation report is clearly linked to its initial external *SAR.*

11.4.5 Screening, awareness and training of *employees*

AML/CFT/CPF Codes of Practice

[COP112] A *supervised person* must keep adequate and orderly records of training provided on the prevention and detection of money laundering, the financing of terrorism, or the financing of proliferation for five years after the end of the calendar year in which the training was provided, including:

- the dates on which training was provided;
- the nature of the training provided;
- names of *Employees* who received the training; and
- records of testing subsequently carried out to measure *Employees'* understanding of the training provided, including pass rates and details of any action taken in cases of failure.

11.5 Access and retrieval of records

Overview

76. The *Money Laundering Order* does not specify **where** records should be kept, but the overriding objective is for *supervised persons* to be able to access and retrieve relevant information **without unreasonable delay**.

AML/CFT/CPF Codes of Practice

[COP113] A *supervised person* must keep documents, data or information obtained under *identification measures* in a way that facilitates ongoing monitoring of each *business relationship*.

[COP114] For all other purposes, the records kept by a *supervised person* must be readily accessible and retrievable by the person. Unless otherwise specified, records relating to evidence of identity, other *CDD* measures, and transactions must be accessible and retrievable **within 5 working days** (whether kept in or outside of Jersey), or such longer period as agreed with the *JFSC*. Other records must be accessible and retrievable **within 10 working days** (whether kept in or outside of Jersey), or such longer period as agreed with the *JFSC*.

[COP115] A *supervised person* must periodically review the condition of paper and electronic records and consider the adequacy of its record-keeping arrangements.

[COP116] A *supervised person* must periodically test procedures regarding access to and retrieval of its records.

[COP117] Records must be maintained in a **readable format**. Where records are kept other than in readable form, they must be maintained such that they can be produced in readable form at a computer terminal in Jersey.

[COP118] When original documents (such as transaction-related vouchers used to input data onto computer systems) that would ordinarily have been destroyed are requested for investigation purposes, a *supervised person* must ascertain whether the documents have in fact been destroyed.

11.5.1 External record-keeping

Overview

77. Where records are kept by another person (group or otherwise), or kept outside Jersey, such as under an outsourcing or storage arrangement, this will present additional factors for a *supervised person* to consider. Regardless of the circumstances, the *supervised person* remains responsible for compliance with all record-keeping requirements.

78. Where an *obliged person* ceases to trade or have a relationship with a *customer* for whom it has provided an assurance to a *supervised person*, particular care needs to be taken to check whether the assurance continues to have effect, or to ensure that evidence of identity is obtained from the *obliged person*. Section 5 of *this Handbook* deals with reliance arrangements made with *obliged persons*.

AML/CFT/CPF Codes of Practice

[COP119] A supervised person must not:

- allow another person (group or otherwise) to keep records; or
- keep records outside Jersey;

where access and retrieval of records (by that person, the JFSC and/or law enforcement) is likely to be impeded by confidentiality or data protection restrictions.

11.5.2 Reorganisation or termination

Overview

79. Record-keeping requirements persist and are unaffected where a *supervised person*:

- merges with another person;
- continues as another person;
- is taken over by another person;

- is subject to internal reorganisation;
- terminates its activities; or
- transfers a block of *customers* (i.e., a "book of business") to another person.

AML/CFT/CPF Codes of Practice

[COP120] A *supervised person* that undergoes mergers, continuance, takeovers or internal reorganisations, must ensure that records remain readily accessible and retrievable for the required periods stated *above*. This extends to the rationalising of computer systems and storage arrangements.

[COP121] Record-keeping arrangements must be agreed with the *JFSC* where a *supervised person* terminates its activities or transfers a block of *customers* to another person.

11.6 Disclosure of records

Overview

80. The *FATF Recommendations* identify several cases where a *financial institution* (or a *DNFBP*) may provide an assurance to another that it will provide documents, data or information:

- *FATF Recommendation* 13 provides that a respondent institution (in the context of a **correspondent banking relationship**) should be able to provide *relevant customer* identification data upon request to the correspondent *financial institution*;
- *FATF Recommendation* 17 provides that a *financial institution* relying upon another party should be required to take adequate steps to be satisfied that relevant documentation relating to *CDD* requirements will be made available by that party upon request and without delay.

81. Accordingly, it is important that where the respondent institution or party relied upon is a *supervised person* in Jersey, there should be no legal impediment to providing the data and information requested.

Statutory requirements (paraphrased wording)

82. *Article 16(7) of the Money Laundering Order states that, where a relevant person (including a person who was formerly a relevant person) (A) has given an assurance under Article 16 of the Money Laundering Order (or under a provision that applies outside Jersey that is equivalent to Article 16 of the Money Laundering Order) to another relevant person (B), Person A must make available to Person B, at Person B's request, evidence of identity that Person A has obtained under Article 3 of the Money Laundering Order. Person A commits an offence under the Proceeds of Crime Law where it fails do so.*

83. *Article 17C(4) of the Money Laundering Order states that, where a relevant person (A) has given an assurance under Article 17C(2)(b) of the Money Laundering Order (or under a provision that applies outside Jersey that is equivalent to Article 17C of the Money Laundering Order) to another person (B), Person A may make available to Person B, at Person B's request, information and evidence of identity that Person A has obtained under Article 3 of the Money Laundering Order. However, A is not required by law to do so.*

84. *Article 19(7) of the Money Laundering Order applies to a relevant person carrying on deposit-taking business (a respondent) who is in receipt of banking services provided by an institution whose address is outside Jersey (a correspondent). It allows the respondent to provide the correspondent with evidence, documents, data and information obtained under Article 3 of the Money Laundering Order on request. However, the respondent is not required by law to provide information to the correspondent.*

11.7 Retention of supporting material for fit and proper determinations for key persons and principal persons, including criminal records certificates

Overview

1. A *supervised person* is required to ensure that its *key persons* and *principal persons* are fit and proper in accordance with Section 10.6 of the Handbook.

2. A *supervised person* is required to maintain documentation concerning the assessment of the fitness and propriety of key persons. This includes criminal records certificates and any other documentation pertaining to these fitness and propriety checks.

Statutory requirements (paraphrased wording)

3. Article 8(1) of the Supervisory Bodies Law gives the JFSC broad powers to carry out its supervisory duties. These include conducting examinations and requiring information from *supervised persons*.

AML/CFT/CPF Codes of Practice

[COP122] A *supervised person* must retain any documents, data, and information relied upon to establish whether a key person or principal person is fit and proper for a period that aligns with their obligations under the relevant data protection legislation and policy.

Part II: SECTOR SPECIFIC GUIDANCE

Industry	**Section**
Trust Company Service Providers (TCSPs)	12
Fund and Security Services Activities	13
Wire Transfers and prepaid cards	14
*AMLSP*s	15
Virtual Asset Service Providers (VASPs)	16
Prescribed Non-Profit Organisations	*No longer contained within this Handbook, refer to guidance on the JFSC website.*

Sections 1 - 11 are applicable to all entities/sectors classified as *supervised persons* and sections 12 – 16 apply to specific Sectors.

12 TRUST COMPANY SERVICE PROVIDERS (TCSPS)

12.1 Overview

1. This section applies to all *supervised persons* who *are TCSPs* as described in the *Guidelines*, including *Trust Company Businesses.* The activity of *TCSP* is described in the *FATF* definition of *Designated Non-Financial Businesses and Professionals (DNFBPs)* which is contained in paragraph 23 of part 3 of Schedule 2 to the *Proceeds of Crime Law,* therefore all TCSPs are *DNFBPs*. TCB is a defined term in Article 2 of the FS(J)L which is directly referenced in paragraph 23 of Part 3 of Schedule 2 to the POC(J)L therefore all those registered as a TCB are also a TCSP but will be referred to as a TCB these have AML/prudential/conduct regulation and supervision. Where a person is a TCSP but not a TCB and therefore has to register under the Proceeds of Crime (Supervisory Bodies) (Jersey) Law 2008.

2. Except for the limited exemption to the Money Laundering Order referred to below all TCSPs (including those regulated as TCBs and not) are *supervised persons* and have to comply with the AML/CFT/CPF obligations set out in this Handbook.

3. Directors who are registered as *TCSPs* and who are not regulated as *TCBs* are considered to be low risk financial services business and certain Articles of the *Money Laundering Order* have been disapplied to them as set out in Proceeds of Crime (Low Risk Financial Services Business) (Jersey) Order 2024 (*Exemption Order*).

4. The purpose of this section is to assist with the application of *identification measures* to a *customer* where a *supervised person* established a *business relationship* or carries out a *one-off transaction* in the course of being a *Trust Company Service Provider.*

12.2 *Identification measures*

5. This section applies where a *supervised person* carries on a business under Article 2(3) of the *FS(J) Law* and, in the course of providing those services, the person provides any of the services specified in Article 2(4) of the *FS(J) Law (a regulated business, namely a Trust Company Business (TCB))*.

6. This section also applies where a *supervised person* carries on a business that is described in paragraph 23(1)(b)(i) of Part 3 of Schedule 2 to the *Proceeds of Crime Law (a Trust company service provider that may include a TCB but may not)*.

7. Directors subject to the *Exemption Order* are not exempt from the obligation to apply *Identification measures.*

8. This section **does not** deal with the provision of any service to a '**COBO-only** fund'. A COBO-only fund is a scheme that would be a collective investment fund (as defined in the *CIF(J) Law*) except for the fact that the capital, the collective investment of which is the object or one of the objects of the scheme or arrangement, is not acquired by means of an offer to the public of *units* for subscription, sale, or exchange.

12.2.1 Obligation to apply *identification measures*

9. Among other things, Article 13 of the *Money Laundering Order* requires a *supervised person* to apply *identification measures*:

› before the establishment of a *business relationship* or before carrying out a *one-off transaction*; and

› in the course of a *business relationship*, where the *supervised person* has doubts about the adequacy of information previously obtained under *identification measures*.

10. A *supervised person* (**Person A**) that provides, acts as or fulfils one or more of the functions listed in Article 2(4) of the *FS(J) Law*, or arranges for another person (**Person B**) to do so (where Person B is an officer or *Employee* of Person A) will be considered to have established a *business relationship* under the *Money Laundering Order*.

11. Where Person B is not an officer or *Employee* of Person A, then Person A will not be considered to have established a *business relationship* each time that it arranges for another person to act as or fulfil such function. However, a *supervised person* will need to consider whether such an arrangement (a transaction) is a *one-off transaction* as defined in Article 4 of the *Money Laundering Order*.

12. A *supervised person* that acts only as a formation agent will not be considered to have established a *business relationship* with its *customer*. However, a *supervised person* will need to consider whether they provide the service of forming a legal arrangement or legal person as a business as defined in Schedule 2, Part 3, paragraph 23 of the *Proceeds of Crime Law.*

13. The requirement to apply *identification measures* also applies where the relationship that a *supervised person* has with its *customer* is conducted through another service provider, e.g., the *supervised person* provides a director to a client company that is administered by another person carrying on *Trust Company Business*.

12.2.2 Information for assessing risk – Stage 1.4

14. This section must be read in conjunction with and is supplemental to, section 3.3.2 of *this Handbook*, which explains how a *supervised person* may demonstrate that it has obtained appropriate information for assessing the risk that a *business relationship* or *one-off transaction* will involve *money laundering,* the *financing of terrorism,* or the *financing of proliferation*.

12.2.2.1 ***Supervised person*** **providing limited services**

Overview

15. Where a *supervised person* provides **only:**

› registered office services; and/or

› secretarial services (defined in this section as **limited services**).

That *supervised person* is unlikely to have any oversight of, or control over, the activities of the legal arrangement or legal person in the way that it would if it also provided one or more directors (or equivalent) or provided full administration services. The absence of oversight or control increases the risk that a legal arrangement or legal person may be used for *money laundering,* the *financing of terrorism,* or the *financing of proliferation*.

16. The presence of this additional risk therefore requires a *supervised person* to request additional information on its *customer*, and on the activities of the legal arrangement or legal person to which it is to provide only limited services, for the purpose of countering *money laundering,* the *financing of terrorism,* and the *financing of proliferation*.

17. The risk that a legal arrangement or legal person may be used for *money laundering,* the *financing of terrorism,* or the *financing of proliferation* is likely to be mitigated where a *customer* to whom only limited services are provided is a body corporate, the securities of which are listed on an *IOSCO* compliant market or on a *regulated market*, or where a *customer* is a *regulated person* (or person who carries on *equivalent business* to any category of *regulated business*).

Guidance notes

18. In the case of a *supervised person* that provides **only** limited services to a legal arrangement or legal person, a *supervised person* may demonstrate that it has obtained appropriate information for assessing the risk that a *business relationship* or *one-off transaction* will involve *money laundering,* the *financing of terrorism,* or the *financing of proliferation* where it collects (at the time that a limited service is first provided and then on an ongoing basis thereafter) information on activities by reference to:

- copies of minutes of directors' and members' meetings that must be kept by a company (including, in the case of a *PCC*, copies of minutes of directors' and members' meetings of the cell company and each of its cells) under Part 15 of the *Companies Law* (or equivalent for other legal persons or legal arrangements); and
- copies of accounts that must be prepared by the directors of a company (including, in the case of a *PCC*, copies of accounts that must be prepared by the directors of the cell company and each of its cells) under Part 16 of the *Companies Law* (or equivalent for other legal persons or legal arrangements); or
- where accounts are not required to be prepared, underlying financial records that are maintained by the directors of that company (or equivalent for other legal persons or legal arrangements).

12.2.2.2 Co-trustees and additional general partners

Overview

19. In some cases, an *express trust* or limited partnership may have more than one trustee or general partner respectively. In such cases, it will be necessary for a *supervised person* that is to act as trustee or general partner to obtain information on each co-trustee or additional general partner (or limited partner that participates in the management of the limited partnership) to fully consider *money laundering, financing of terrorism,* and *financing of proliferation* risk.

Guidance notes

20. A *supervised person* that is to act as a trustee of an *express trust* may demonstrate that it has obtained appropriate information for assessing the risk that a *business relationship* or *one-off transaction* will involve *money laundering,* the *financing of terrorism,* or the *financing of proliferation* where it collects information on any co-trustees of the trust.

21. A *supervised person* that is to act as a general partner of a limited partnership may demonstrate that it has obtained appropriate information for assessing the risk that a *business relationship* or *one-off transaction* will involve *money laundering,* the *financing of terrorism,* or the *financing of proliferation* where it collects information on any additional general partners or limited partners that participate in the management of the limited partnership.

22. The information requested may include why it is necessary to have more than one trustee or general partner, and the stature and regulatory track-record of the co-trustee or additional general partner.

12.2.3 Assessment of risk – Stage 2.1

Overview

23. This section must be read in conjunction with and is supplemental to section 3.3.4 of *this Handbook*, which sets out several factors that are to be taken into account by a *supervised person* when assessing the risk that a *business relationship* or *one-off transaction* will involve *money laundering,* the *financing of terrorism,* or the *financing of proliferation*.

Guidance notes

24. A *supervised person* that is a TCSP may demonstrate that it has assessed the risk that a *business relationship* or *one-off transaction* will involve *money laundering*, the *financing of terrorism*, or the *financing of proliferation* where it considers the following additional risk factors:

› any failure on the part of a *customer* to be open about the *source of funds*. In the case of a trust, this could indicate that, for example, a settlor is in fact a "dummy" settlor who is using another's funds and not their own;

› any failure to be open about the purpose and intended nature of the *business relationship* or *one-off transaction*. In the case of a trust, this could indicate that, for example, a settlor is withholding information on the persons who are actually intended to benefit from the trust, e.g., a settlor only nominates charities as beneficiaries of a trust, but they do not intend that the charity will in fact benefit (known as a "blind" trust);

› any request to include unusual or non-standard clauses in a trust instrument or other constitutional document that might indicate that the disclosed purpose of the structure is not genuine; and

› any request for unusually close supervision or control of assets by a person other than the *supervised person*.

12.2.4 *Identification measures*: Finding out identity and obtaining evidence

Overview

25. The meaning of *identification measures* within *this Handbook* is set out in the Glossary *of this Handbook*. *Identification measures* include determining who the *customer* is.

26. Where a *supervised person* is to act as the trustee of an *express trust*, *customers* will include the settlor, protector (if any), beneficiaries with a vested right and any other beneficiaries and persons who are the object of a power and that have been identified as presenting a higher risk (see section 1.1.1.1 of *this Handbook*).

27. Where a *supervised person* is to act as the general partner of a limited partnership, *customers* will include the limited partners of the partnership (see section 1.1.1.1 of *this Handbook*).

28. Where a *supervised person* is to provide a non-management service, such as registered office, in respect of a limited partnership, the *customer* will be the general partner acting for the limited partnership – a third party (see section 4.3.3 of *this Handbook*).

29. Where a *supervised person* is to provide a service to a company, the *customer* will be the company (see section 4.5.1 of *this Handbook*).

30. Where a *supervised person* is to provide a service to a foundation, the *customer* will be the foundation (see section 4.5.3 of *this Handbook*).

31. Where a *supervised person* is to provide a service to a separate limited partnership, incorporated limited partnership or limited liability partnership, the *customer* will be the partnership (see Section 4.5.5 of *this Handbook*).

32. Where a *supervised person* is to form a company, partnership or foundation, the *customer* will be the persons who are the *Beneficial owners and/or controllers* of the legal person (see sections 4.2.2 and 4.5 of *this Handbook*).

12.2.4.1 Finding out identity – Legal arrangement that is a trust

Guidance notes

33. A *supervised person* that is to act as the trustee of an *express trust* may demonstrate that it has applied *identification measures* under Article 3(2)(a) of the *Money Laundering Order* to its *customer*, where it applies those measures to:

› the settlor, including any person subsequently settling funds into the trust (except if deceased) and any person who directly or indirectly provides trust property or makes a testamentary disposition on trust or to the trust;

› any co-trustee;

› any protector;

› any beneficiary with a vested right;

› any other beneficiary or person who is the object of a power and that has been identified as presenting a higher risk; and

› any other person exercising **ultimate effective control** over the trust.

34. In any case where a settlor, protector, beneficiary, object of a power or other person referred to in paragraph 30 (the **person**) is not an individual, a *supervised person* may demonstrate that it has identified each individual who is the person's *Beneficial owner and/or controller* under Article 3(2)(c)(iii) of the *Money Laundering Order* where it has identified:

› each individual with a **material controlling ownership interest** in the capital of the person (through direct or indirect holdings of interests or voting rights) or who exerts **control through other ownership means**;

› to the extent that there is doubt as to whether the individuals exercising control through ownership are *Beneficial owners*, or where no individual exerts control through ownership, any other individual exercising **control** of the person **through other means**;

› where no individual is otherwise identified under this section, individuals who **exercise control** of the person **through positions held** (e.g., those who have and exercise strategic decision-taking powers or have and exercise executive control through senior management positions).

35. For lower risk relationships, a general threshold of 25% is considered to indicate a **material controlling ownership interest** in the capital of the person. Where the distribution of interests is uneven, the percentage where effective control may be exercised (a material interest) may be less than 25% when the distribution of other interests is considered, i.e., interests of less than 25% may be material interests.

12.2.4.2 Finding out identity – Legal arrangement that is a charitable trust (capital markets)

Guidance notes

36. A *supervised person* that is to act as the trustee of a charitable trust which is established to hold an investment in a security-issuing vehicle, or to hold security (as bare trustee for security-holders) over assets held within such a vehicle, may demonstrate that it has applied *identification measures* under Article 3(2)(a) of the *Money Laundering Order* to its *customer*, where it applies those measures to:

- › the originator or instigator of the capital market transaction; and
- › each security-holder that can exercise **effective control** over the underlying security-issuing vehicle.

12.2.4.3 Obtaining evidence of identity – Legal arrangement that is a trust

Overview

37. The measures that must be applied to obtain evidence of identity of beneficiaries and persons who are the object of a power and that have been identified as presenting higher risk will reflect the verification methods that are available at a particular time to the trustee. For example, it may not be appropriate to request evidence directly from the beneficiary or object of a power.

38. Where a *supervised person* is not familiar with a document obtained as evidence of identity, additional appropriate measures may be necessary to satisfy itself that the evidence is genuine.

AML/CFT/CPF Codes of Practice

[COP123] All key documents (or parts thereof) obtained as evidence of identity must be in a language understood by the employees of the business and must be translated into English at the request of the *FIU* or of the *JFSC*.

12.2.4.4 Finding out identity – Legal arrangement that is a limited partnership

Guidance notes

39. A *supervised person* that is to act as the general partner of a limited partnership may demonstrate that it has applied *identification measures* under Article 3(2)(a) of the *Money Laundering Order* to its *customer* where it applies those measures to limited partners holding a **material controlling ownership interest** in the capital of the partnership (through holdings of interests or voting rights) or any other person exercising **control through other ownership means**, e.g. partnership agreements, power to appoint *senior management*, or any outstanding debt that is convertible into voting rights.

40. To the extent that there is doubt as to whether the persons exercising control through ownership are *Beneficial owners*, or where no person exerts control through ownership, a *supervised person* that is to act as the general partner of a limited partnership may demonstrate that it has applied *identification measures* under Article 3(2)(a) of the *Money Laundering Order* to its *customer* where it applies those measures to any other person exercising **control** over the partnership **through other means**, e.g., those who exert control through personal connections, by participating in financing, because of close family relationships, historical or contractual associations or as a result of default on certain payments.

41. Where no person is identified under this section, a *supervised person* that is to act as the general partner of a limited partnership may demonstrate that it has applied *identification measures* under Article 3(2)(a) of the *Money Laundering Order* to its *customer* where it applies those measures to persons who exercise **control through positions held** (e.g. those who have or exercise strategic decision-taking powers or have or exercise executive control through senior management positions, e.g. general partner or limited partner that participates in management).

42. In any case where a partner or other person is not an individual, a *supervised person* may demonstrate that it has identified each individual who is that person's *Beneficial owner and/or controller* under Article 3(2)(c)(iii) of the *Money Laundering Order* where it has identified:

› each individual with a **material controlling ownership interest** in the capital of the partnership (through direct or indirect holdings of interests or voting rights) or who exerts **control through other ownership means**;

› to the extent that there is doubt as to whether the individuals exercising control through ownership are *beneficial owners*, or where no individual exerts control through ownership, any other individual exercising **control over the partnership through other means**; and

› where no individual is otherwise identified under this section, individuals who exercise **control** of the partnership **through positions held** (e.g., those who have and exercise strategic decision-taking powers or have or exercise executive control through *senior management positions*).

43. For lower risk relationships, a general threshold of 25% is considered to indicate a **material controlling ownership interest** in the capital of a limited partnership. Where the distribution of interests is uneven, the percentage where effective control may be exercised (a material interest) may be less than 25% when the distribution of other interests is considered, i.e., interests of less than 25% may be material interests.

12.2.4.5 Obtaining evidence of identity – Legal arrangement that is a limited partnership

44. Where a *supervised person* is not familiar with a document obtained as evidence of identity, additional appropriate measures may be necessary to satisfy itself that the evidence is genuine.

AML/CFT/CPF Codes of Practice

[COP124] All key documents (or parts thereof) obtained as evidence of identity must be in a language understood by the employees of the business and must be translated into English at the request of the *FIU* or of the *JFSC*.

12.2.4.6 Finding out identity – Legal person that is a PCC

Overview

45. This section must be read in conjunction with and is supplemental to sections 4.5.1 and 4.5.2 of *this Handbook*.

46. Under Article 127YDA(1) of the *Companies Law*, in the case of both *PCCs* and *ICCs*, a cell shall have the same registered office and secretary as the cell company. The registered office must also be in Jersey.

47. As a result, where a *supervised person* provides a registered office or secretary to a *PCC,* **it will do so for each cell of that *PCC* as well**. Because the cell of a *PCC* does not have the ability to enter into arrangements or contract in its own name, for the purposes of Article 3 of the *Money Laundering Order*, the *PCC* will be taken to be a *customer* acting for a third party and each cell will be taken to be a third party that is a person other than an individual. *Identification measures* must therefore be applied under Article 13 of the *Money Laundering Order* to the ***PCC*** (the *customer*) and **each cell** of the *PCC* (a third party).

12.2.5 Timing of *identification measures*

48. This section must be read in conjunction with and is supplemental to sections 4.1 and 4.7 of *this Handbook*.

49. In line with Article 13(8) of the *Money Laundering Order*, a *supervised person* that is to act as a trustee may delay obtaining evidence of the identity of a *customer* after the time that a *business relationship* is established so long as:

› it obtains evidence of identity at the time of, or before, distribution of trust property or income; and

› it is satisfied that there is little risk of *money laundering,* the *financing of terrorism,* or the *financing of proliferation* occurring because of obtaining evidence after entitlement is conferred.

50. Similar provisions should apply in a case where the *customer* of the *supervised person* changes during the course of a *business relationship*.

Guidance notes

51. During a *business relationship*, a *supervised person* that is the trustee of an *express trust* may demonstrate that it has obtained evidence that is reasonably capable of verifying the identity of each beneficiary with a vested right where:

› it obtains evidence of identity at the time of, or before, distribution of trust property or income; and

› it is satisfied that there is little risk of *money laundering*, the *financing of terrorism, or the financing of proliferation* occurring because of obtaining evidence after entitlement is conferred.

52. During the course of a *business relationship*, a *supervised person* that is the trustee of an *express trust* may demonstrate that it has obtained evidence that is reasonably capable of verifying the identity of a beneficiary or person who is the object of a trust power, where it does so at the time that the person is **identified as presenting a higher risk**.

12.2.6 Failure to complete *identification measures*

53. This section must be read in conjunction with and is supplemental to section 4.8 of *this Handbook*.

54. Under Article 14 of the *Money Laundering Order*, if a *supervised person* is unable to apply *identification measures* when required to do so, then it must terminate that *business relationship* or not carry out that *one-off transaction* and consider whether to make a *SAR* to the *FIU*.

55. This requirement may cause conflicts where a *supervised person* is acting as a trustee, its *customer* is the beneficiary or object of a power of a trust and:

- the relationship between a *supervised person* and its *customer* is governed by other legislation, e.g., the [Trusts (Jersey) Law 1984;]() and
- the termination of a relationship with a *customer* (a beneficiary or object of a power) may have a prejudicial effect on the interests of other *customers*.

56. This requirement may also cause conflicts where a *supervised person* is acting as a council member, its *customer* is a foundation, and the foundation is governed by the *Foundations Law*. Under Article 12(3) of the *Foundations Law* the retirement or removal of the qualified member of a foundation does not take effect until **immediately before** the appointment of a new qualified person to be the qualified member of the council has taken effect.

57. In order to address such potential issues, termination of a *business relationship* may be **delayed** until such time as compliance with Article 14 of the *Money Laundering Order* does not conflict with another legal requirement, and/or does not have any prejudicial effect on the interests of other *customers*, so long as the risk of *money laundering,* the *financing of terrorism,* or the *financing of proliferation* is effectively managed.

12.2.7 Provision of information by trustees

Statutory requirements (paraphrased wording)

58. *Article 2 of the Information Order requires a person who is acting as a trustee of a trust to state that that person is acting in their capacity as trustee of that trust (and not in that person's personal capacity) when:*

- *forming a business relationship with a relevant business; or*
- *conducting a one-off transaction with a relevant business.*

59. *Article 3(1) of the Information Order states that despite any provision of any trust document, or any other enactment, the trustee of a trust:*

- *must provide to a competent authority any information requested by that competent authority; and*
- *may provide to a relevant business with which the trust has a business relationship, on request by that business, information regarding:*
  - *the beneficial ownership of the trust;*
  - *the settlor, protector or enforcer of the trust, if any; or*
  - *the assets of the trust that are to be held or managed by the relevant business under the terms of the business relationship.*

60. *Article 3(2) of the Information Order states that a request for information by an external competent authority must be made via a competent authority under an appropriate international co-operation request.*

61. *Article 3(3) of the Information Order states that on receipt of a request for information from an external competent authority under paragraph (2), a competent authority may request all or any of that information from the trust.*

13 *FUND* AND SECURITY SERVICES ACTIVITIES

13.1 Overview of section

1. This section is supplemental to and should be read in conjunction with the sections of *this Handbook* referenced in the text below.

2. The purpose of this section is to assist with the application of *CDD*, the conduct of risk assessments and additional *AML/CFT/CPF* requirements by funds, securities issuers and their service providers. The definition of *financial services business* in the *Proceeds of Crime Law* means that:

   a. **regulated** and **prudentially supervised** funds and fund service providers under the *CIF(J) Law* and the *FS(J) Law*;

   b. funds that are not regulated (such as unregulated funds under the Collective Investment Funds (Unregulated Funds) (Jersey) Order 2008 and private funds) and their service providers; and

   c. other securities issuers and their service providers,

   are subject to the same statutory requirements in the *Money Laundering Order*. Further guidance is available in sections 3.1, 3.2, 3.3 and 3.12 of the *Guidelines.*

3. The types of funds, securities issuers and their service providers to which this section applies are described in the *Guidelines*. For the purposes of this section references to a fund include all sub funds and constituent parts of the fund.

4. It should also be noted that funds, securities issuers and their service providers might be conducting other types of *financial services business,* e.g., a service provider that is a trustee to a fund will also be a *TCSP* for **the** purposes of Schedule 2 of the *Proceeds of Crime Law.*

5. Every *supervised person* has obligations pursuant to the *Money Laundering Order*. Where there are several different service providers involved in a fund or securities issuer structure their respective *CDD* obligations and subsequent *CDD* measures applied may differ. The differences may be attributable to different roles, risk appetites and risk assessments, which will determine how they fulfil their *AML/CFT/CPF obligations*.

6. The service providers of funds or securities issuers can include all those entities and activities listed in Schedule 2, Part 2, paragraph 9 of the *Proceeds of Crime Law*. The list below provides some examples of roles that *supervised persons* may hold with a fund or securities issuer as their *customer*. As noted in paragraph 5 above, different *supervised persons* may have varying *CDD* obligations based on the type of service they provide to a Fund:

- Auditor;
- Administrator/Registrar;
- Manager;
- Investment Adviser;
- Lender;
- Class G Director;
- Asset Manager;
- Distributor;

- › Custodian;
- › Legal Adviser.

7. Natural Persons such as Class G Directors regulated under the *FS(J) Law* are *supervised persons* and will also have *AML/CFT/CPF obligations*. The *JFSC* has produced the *Guidance note* Natural persons carrying on a single class of trust company business for these individuals.

8. An entity that is a **Managed Entity** (meaning an entity that is managed by a Manager of a Managed Entity registered to carry on class ZK of fund services business under the *FS(J) Law* has the same *AML/CFT/CPF obligations* as any other Fund Operator. The *JFSC* has produced a *Guidance note:* Manager of managed entity (MoME) and certain managed entities.

9. Funds, securities issuers, and their service providers may have different *AML/CFT/CPF obligations*. For example, any one of the service providers in the list above may be neither a Jersey legal person or arrangement nor carrying on business in or from within Jersey and so will not be a *supervised person* and will not be subject to Jersey *AML/CFT/CPF obligations*. A fund, securities issuer and/or their service provider that is not a *supervised person* may have *AML/CFT/CPF obligations* in another jurisdiction. A non-Jersey service provider that is not subject to Jersey *AML/CFT/CPF obligations* may act for a Jersey fund, such as a Jersey fund company, that **does** have Jersey *AML/CFT/CPF obligations*. For the remainder of this section the term “securities issuer” will be used, which includes both “funds” and “securities issuers”.

13.2 *AML/CFT/CPF* risk assessments

13.2.1 Overview – Obligation to conduct risk assessments

10. To meet its *AML/CFT/CPF obligations*, a *supervised person* is required to prepare a *BRA*, along with a *CRA* for each of its *customers*. These obligations are covered in sections 2.3 and 3.3.2 of *this Handbook* respectively. The *BRA* and *CRA* may be completed differently based on what the *supervised person* is/does, for example:

Supervised person	***BRA***	***CRA***
Administrator as service provider.	Administrator’s business.	Securities issuers for which the administrator acts.
Securities issuer.	Securities issuer itself.	Investors.

11. All the *financial services businesses* defined by the *Proceeds of Crime Law* that are *supervised persons* under the *Money Laundering Order* must conduct a *BRA* and individual *CRAs*. Where the conducting of a *BRA*/*CRA* is outsourced to an external party, the *supervised person* must take adequate steps to ensure the *BRA* and *CRA* are properly conducted and documented.

Guidance notes

12. For *supervised persons* who are subject to one or more of the *Codes of Practice* published by the *JFSC* (such as the Trust Company Business Code of Practice) there is also an obligation for a wider, operational *BRA* to be conducted. When preparing a *BRA* or *CRA*, factors in this operational *Business Risk Assessment* may be relevant. Therefore, a combined *BRA* and operational *Business Risk Assessment* may be appropriate.

13. Risks that are not normally considered to be *AML/CFT/CPF*-specific may also be relevant to a *BRA*, for example, credit risk, tax risk, investor eligibility risk, cyber security related risk etc.

14. It is common practice for a securities issuer to outsource the conduct of its *BRA* to an administrator. In such circumstances, the administrator will also need to conduct a *CRA* on the securities issuer (its *customer*) as it has two separate roles - acting both for itself (conducting a *BRA* on itself and *CRA* on the securities issuer) and as delegate for the securities issuer (conducting a *BRA* and *CRA* on behalf of the securities issuer). Although there may be similar factors considered in the *BRA* and the *CRA*, separate assessments will need to be conducted and documented.

13.2.2 BRA

Overview

15. This section is supplemental to and should be read in conjunction with section 2.3 of *this Handbook* regarding *BRAs*.

Guidance notes

16. When conducting a *BRA* there may be several parties involved in the creation of a securities issuer and the conduct of the securities issuance business – in such circumstances, the *AML/CFT/CPF* risks arising from the involvement of all parties will need to be considered.

17. *Supervised persons* should satisfy themselves that sufficient information has been obtained in relation to a securities issuance structure to fully understand the structure and manage the risk of being involved with the proceeds of criminal conduct (or property used in or intended to be used in criminal conduct). This may include the securities issuer itself being set up for a fraudulent purpose or the securities issuer being used to facilitate *money laundering*. Not all these potential factors will be applicable in every case, e.g., there may be no external finance.

18. Potential factors to consider when conducting a securities issuer's *BRA* may include but are not limited to those set out in the table below. This list is not exhaustive, and the *supervised person* will need to consider the risks relevant to them:

Securities issuer (including a fund)	
Type of securities issuer	› Open/closed › Public/private › Regulated/unregulated › Listed/unlisted › Asset Class - Private equity/venture capital/property/hedge fund/fund of funds.
Rationale for securities issuer	› Does fund/securities issuer proposal make sense in light of the objective? › Capital accumulation/income producing/both.
Jurisdiction/Domicile of securities issuer	› Local/non-domiciled.
Securities issuer's structure	› Legal Structure: Limited partnership/ company/unit trust/*ICC*/*PCC*/incorporated limited partnership /separate limited partnership › Separate *Governing body*, i.e., general partner/trustee › Complex/Simple › *SPVs* to hold assets › Part of platform of the manager of the securities issuer › Umbrella.

Securities issuer (including a fund)	
Conflict(s) of interest	› Promoter v securities issuer investors › Securities issuer service providers v Securities issuer investors › Related parties v securities issuer investors › Between Investors (evidenced in some cases by side letters) › Between securities Issuer service providers.
Unusual features	› Lock ins › Asset holding arrangements › In specie contributions.
Influential persons	› The entities named in the list at paragraph 6 above › Promoter › Investment Committee – powers, composition, independence › Consultants – value for money, related? › Valuers – independent? › Suppliers › *SPV* level suppliers › Letting agents › Asset managers › Developers › Legal advisers › Tax advisers › Auditors › Co-investors › Key investors/Seed investors.
Risk indicators	› *PEPs* › High risk jurisdictions › Sanctions- check Sanctions designations lists.
Cash flow	› In specie payments/redemptions permitted? › Third party payments permitted? › Early redemptions permitted? › Budgetary and payment controls of monies flowing out of securities issuer.

19.

Investors/Target market	
Type	› Retail › Professional / financially sophisticated › Institutional › Co-investors at issuer level or at investment level (see paragraph 26 below).

Investors/Target market	
Method of distribution/Solicitation	› Word of mouth /club arrangement/reverse solicitation/ private distribution / public distribution › Control of raising money and distribution of securities › Distributor employed › Promoter distributes › In house securities issuer (i.e., bank for high-net-worth clients) › Investment adviser distributes › Subject to local marketing requirements, e.g., Alternative Investment Fund Managers Directive?
Investor's holding method	› Via intermediaries › Via nominee › Directly/indirectly › Complexity of holding structure › Rationale for holding structure.
Investor information	› *Source of funds* › *Source of wealth* › Rationale.

20.

Investments	
Type/Asset class	› Property/private equity/hedge fund/fund of funds/ infrastructure etc. › Liquid/illiquid assets.
Listed/Unlisted	› Recognised market?
Risks associated with that asset class	› Diamonds/ gold /luxury goods – higher *AML/CFT/CPF* risk › Have securities issuer and securities issuer service providers sufficient knowledge and competence to deal with the asset class?
Valuation	› Listed assets easier to value › Specialist assets may be difficult to value › Independent valuer - Experts linked already to the fund?
In specie receipt/payment	› Valuation › Title transfer effective? › Liquid/illiquid › Related party transferring the asset?
Sanctions	› Check the Sanctions designations lists.

21.

Factors common to securities issuer service providers, *Governing body*, finance provider, Investors/target market, instigator/promoter/creator	
Stature	› Public/Private › Newly established/long established › Listed/unlisted › Global/local/number of jurisdictions/number of offices.
Legal form	› Legal person/legal arrangement.
Ownership and control	› Wide spread of ownership/control or sole ownership › Dominant directors/shareholders.
Regulatory status	› Regulated/unregulated.
Reputation	› Subject to regulatory or other disciplinary actions › Subject to legal action › International/National reputation › Held in high regard in business community.
Track record	› Relevant experience particularly in the case of specialist securities issuers or those perceived to be high risk, for example, futures and options funds.
Jurisdiction	› Local/non-domiciled › Multiple jurisdictional operations › Multiple branches/regional office.
Solvency	› Insolvency proceedings › Judgements › Issues with accounts (audit) › Lack of liquidity.
Risk indicators	› *PEPs* - Are there are any? › Sanctions - Have they been checked? › High risk jurisdictions – are there links?

22.

Instigator/Promoter/Creator	
Control of securities issuer	› Participation in structure – owns management shares, owns *Governing body*, is investment manager/adviser/directors on board of *Governing body*.

23.

Securities issuer service providers (including **fund operators**)	
General	› Risks in relation to fund operator role or that particular securities issuer › Sub outsourcing.

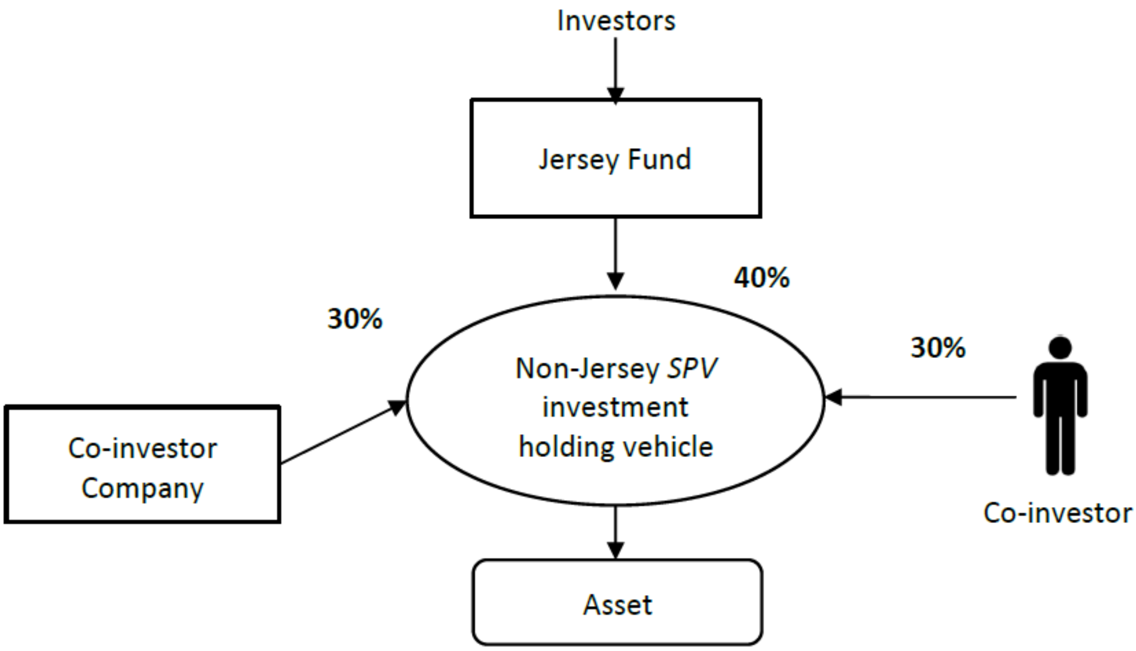
24.

Governing body	
Control	› Independent/equal/proportionate dominant individuals › Bank account mandates.
Corporate governance	› Compliance culture, compliance monitoring policy › Frequency that *policies and procedures* are updated.

25.

Finance	
Source of borrowing	› Regulated bank/credit institution › Private finance – where are funds from? › Layers of borrowing- how many lenders? › Related party?
Structure	› Loan › Bond › Ring fencing › Priority.
Security	› Secured/unsecured › Collateral › Limited recourse › Guarantor › Take title › Can lender deal with the asset it is holding as security?
Level of borrowing	› Securities issuer › *SPV.*
Rationale	› Make sense? › Normal commercial terms? › Unusual features?
Onward lending	› Why? › Who to? › Benefit to the securities issuer?

26. An example of a factor to consider in a securities issuer *BRA* is the existence of co-investors – see the diagram below:



27. The non-Jersey *SPV* investment holding vehicle is not a *supervised person* so has no Jersey *AML/CFT/CPF obligations*.

28. The securities issuer's *BRA* should consider the *AML/CFT/CPF* risks arising from the existence of the co-investors in the structure. These risks may include (but are not limited to) connections to a jurisdiction listed in Appendix D2 of *this Handbook* or whether the co-investor or the ultimate *beneficial owner* of the co-investor company is a *PEP*. Sufficient information should be obtained to assess the *AML/CFT/CPF* risks in this aspect of the business.

13.2.3 *CRA* – risk indicators

29. This section is supplemental to and should be read in conjunction with section 3.3.4 of *this Handbook*.

30. The lists below provide examples of potential risk indicators and are not exhaustive. The results of any national risk assessment or similar must also be considered. The presence of one or more low or high-risk indicators does not necessarily mean a *customer* is low or high risk, and their rating needs to be assessed on a **case-by-case basis**. Risk will be assessed at initial take-on of a *customer* but will also need to be reviewed on a regular basis and at trigger events, to ensure the risk rating remains appropriate.

31. Consideration should also be given to whether it is appropriate to on-board a *customer* at all, and whether a *SAR* should be submitted.

32. Potential higher risk indicators at take-on of a *customer* (securities issuer or investor).

Where the *customer*:

- has provided information/documentation that cannot be verified;
- has links to a *PEP*;
- has links to a *higher risk country or territory;*
- is evasive/inconsistent when additional information is requested such as regarding identity of *Beneficial owners and/or controllers/source of funds*/purpose and expected transactions;

- has a complex structure, for example, operates via layers of representatives making identification difficult;
- is revealed to have money problems (i.e., debt judgements);
- is the subject of regulatory or criminal actions or has associates with these characteristics;
- acts as a nominee and there is an unwillingness to identify the underlying third party;
- is an *NPO*/Charity that might be susceptible to abuse regarding terrorist activities such as medical and emergency relief charities with an unlimited global scope. Or where an *NPO*/Charity operates in a specific geographical area but then transfers monies to a country/territory/jurisdiction not within the specific geographical area;
- is a securities issuer and:
  - is aiming to invest in products that may be susceptible to *money laundering*, for example diamonds and gold;
  - has a one-off minimum investment amount so that it operates below *AML* reporting threshold amounts;
  - is a highly liquid open-ended fund (the *customer*) with the possibility of frequent subscriptions and redemptions;
  - uses unregulated securities issuer service providers;
  - outsources functions without any valid reasons provided;
  - has a complex structure so it is difficult to ascertain who the underlying beneficiary is, for example using many *SPV*s and intermediaries.

33. Potential higher risk Indicators that may be flagged during ongoing monitoring of the *customer* (securities issuer or investor).

Where the securities issuer:

- has entered or intends to enter into finance arrangements that are either at a higher rate or lower rate than usual with no rationale provided;
- has or intends to purchase assets without independent valuations (particularly from connected persons);
- receives or sends monies to related or unrelated third parties that do not fit the pattern of transactions expected for the securities issuer and no acceptable rationale is provided;
- transfers monies to *SPV*s which the securities issuer's *customer* appears to have no control over;
- purchases assets without proof of title from the seller and title to the assets is not clearly transferred to the securities issuer's *customer*;
- engages consultants who add little benefit and receive high fees (particularly in countries associated with a higher risk of corruption);
- enters into a promise to purchase agreements for which monies are paid where transactions are regularly aborted, resulting in forfeiture of the monies;
- is investing with no obvious commercial rationale and is inconsistent with the securities issuer's *customer* profile;
- regularly pays fees, commissions and costs to source and investigate transactions, but no transactions are executed;

- exhibits transaction activity that does not follow the expected pattern or changes substantively with no rational explanation;
- displays endemic conflicts of interest;
- regularly changes bank accounts and uses different securities issuer service providers in different jurisdictions.

Where the investor:

- requires a high level of liquidity and indicates funds may need to be withdrawn/moved at short notice;
- is proposing an investment of an unexpected large amount.

13.2.4 Risk assessments for SPV Governing bodies

34. Issuer service provider to conduct a *CRA* on each of its *customers*, i.e., the investors. Securities issuer ***SPV Governing body*** is a vehicle established for the specific purpose of acting as the *Governing body* of a securities issuer. Common examples are a company established to act as the general partner of a limited partnership which is a securities issuer or a trustee of a unit trust which is a securities issuer.

35. A unit trust or a limited partnership has no separate legal personality, so the *SPV Governing body* is the *customer* of the securities issuer service provider (see Article 3(2)(a) and (c) of the *Money Laundering Order*). However, trustees and general partners are also securities issuer service providers. Effectively they have two capacities - they are both a securities issuer service provider and a securities issuer *Governing body*. For the purposes of this section if a trustee or general partner provides services to **more than one** securities issuer it will not be regarded as an *SPV* but will be regarded as a securities issuer service provider.

36. In these circumstances, its *BRA* and *CRA* conducted as securities issuer service provider and the *BRA* it conducts in its capacity as *SPV Governing body* of the securities issuer are likely to significantly overlap. To avoid duplication of effort, it may be appropriate to consolidate these 3 Risk Assessments, provided that all relevant risks (i.e., of all 3 risk assessments) are appropriately considered. This has no effect on the separate obligation of the securities.

Entity	***BRA***	***CRA***	**Entity**	***BRA***	***CRA***
Non *SPV* trustee of unit trust as securities issuers.	Self.	Securities issuer.	*SPV* trustee of one unit trust as securities issuer.	Consolidated risk assessment combined *BRA*/*CRA* for trustee and securities issuer *BRA* as *SPV* trustee is intrinsically part of the securities issuer.	
Unit trust.	Self.	Investors.	Unit trust.	See above.	Investors.

37. Left intentionally blank.

13.2.5 Documenting risk assessments

Securities issuers

Overview

38. This section is supplemental to and should be read in conjunction with section 3 and section 2 of *this Handbook*.

39. *Supervised persons* are required to ensure their *BRAs* and *CRAs* are properly documented.

Guidance notes

40. Comprehensive subscription agreements/investor questionnaires may assist in obtaining information on a securities issuer's investors and provide sufficient detail to enable the securities issuer to carry out a *CRA*. However, a subscription agreement/investor questionnaire **is not** a replacement for a *CRA*.

41. For certain types of products or services, standard *customer* profiles may assist the *CRA* process. In such cases, the *supervised person* will need documented procedures which consider:

› whether the intention is to only accept investors who fit the standard *customer* profile.

› if not, how will exceptions to the standard *customer* profile be managed, either at the outset or subsequently?

› whether (for instance) individual *CRAs* will be conducted with respect to any *customers* that do not fit the standard *customer* profile.

42. The *supervised person* always remains ultimately responsible for its risk assessments regardless of whether they outsource the conduct of them to another party.

13.3 *Customer identification measures*

Overview

43. Section 3 of *this Handbook* describes the stages of the identification process and provides guidance in relation to each stage. *CDD* is not limited to finding out the identity of the *customer* and obtaining verification (e.g., taking their personal details and copies of their passport and driving licence). The table below (explained in further detail at section 3.3 of *this Handbook*) summarises *CDD* requirements:

<table>
<tr><th>CDD element</th><th colspan="2">Activity</th></tr>
<tr><td rowspan="8">Identification measures</td><td colspan="2">Risk assessment.</td></tr>
<tr><td colspan="2">Identify customer.</td></tr>
<tr><td colspan="2">Identify third parties.</td></tr>
<tr><td>Identify person acting for customer.</td><td>Verify authority to act.</td></tr>
<tr><td rowspan="2">Where customer not individual:</td><td>Understand ownership/control structure.</td></tr>
<tr><td>Identify Beneficial owners and/or controllers.</td></tr>
<tr><td colspan="2">Obtain information on purpose/nature.</td></tr>
<tr><td style="display:none"></td></tr>
<tr><td rowspan="2">Ongoing monitoring</td><td colspan="2">Scrutinising transactions/activity.</td></tr>
<tr><td colspan="2">Keep documents/information up to date.</td></tr>
</table>

44. The following sections provide guidance on the identification of *customer*s, ultimate Beneficial owners and third parties. These sections must be read in conjunction with the referenced sections of *this Handbook*.

13.3.1 Obligation to apply *identification measures*

Overview

45. Section 3.1 of *this Handbook* states that a *customer* may be an individual (or a group of individuals) or a legal person. Further guidance on finding out identity and obtaining evidence of identity is provided at the following sections:

***AML/CFT/CPF Handbook* Section**	**Type of *customer***	**Securities issuer structure**
4.3	Individual/group of individuals.	
4.5	Legal person.	› Company. › Limited liability partnership. › Separate limited partnership. › Incorporated cell.
4.4	Individual or legal person acting for a legal arrangement.	› Trustee on behalf of a unit trust. › General partner on behalf of a limited partnership.

46. For the purposes of this section, companies, limited partnerships, and unit trusts will be used as practical examples as these are the most common security issuer structures.

47. Each of the security issuer's investors are its *customers*. The investors may take a variety of legal forms and Article 3 of the *Money Laundering Order* specifies how *identification measures* are applied to each.

Securities issuer structure	***Supervised person* re each security issuer structure**	***Customer*/Investor**
Company.	Company.	› Article 3(2)(a) of the *Money Laundering Order* - individual. › Article 3(2)(aa) of the *Money Laundering Order* - any person acting on behalf of the *customer.* › Article 3(2)(b) of the *Money Laundering Order* - acting for a third party (legal arrangement). › Article 3(2)(c) of the *Money Laundering Order* - not an individual but legal person. Legal persons/arrangements apply the Three Tier Test.
Limited partnership.	General partner on behalf of the limited partnership.	
Unit trust.	Trustee on behalf of the unit trust.	

48. The Three Tier Test refers to the process by which a *supervised person* may determine each individual who is a *Beneficial owner and/or controller* and is covered in detail at Section 4 of *this Handbook*. However, it can be summarised as determining the individuals who exercise control through:

› ownership means; and

› other means; or

› through positions held.

When applying the Three Tier Test, if no one is present at Tiers 1 and/or 2, then consider Tier 3. There may be more than one individual at Tiers 1 and/or 2.

49. Section 3.3 of *this Handbook* lists the various steps of the identification process, of which identifying the *customer* is only a part. A *supervised person* must also understand the ownership and control of the *customer* and identify:

› any Beneficial owners and/or controllers of the *customer*;

› those third parties for whom the *customer* acts indirectly/directly (e.g., legal arrangements); and

› others listed in Article 3(2) of the *Money Laundering Order* (which links to Article 3(7) of the *Money Laundering Order* e.g., settlor/protector).

50. The starting point is that the *supervised person* has to determine who everyone detailed in paragraph 49 above is, as part of its *identification measures*.

Guidance notes

51. Responsibility for applying *CDD* measures (which includes *identification measures* and ongoing monitoring) rests with the ***Governing body*** of the securities issuer, as detailed in the table below:

Type of security issuer entity	**Responsibility**
Company.	Directors.
Limited partnership/Unit trust.	Directors of the general partner/trustee of the limited partnership/unit trust where the general partner/trustee is a company.
Protected cell.	Directors of the *PCC*, not each of the protected cells, although the directors of the protected cells may assist with compliance.
Incorporated cell.	Directors of each of the incorporated cells.

13.3.2 *Identification Measures* - Securities issuer service provider

Guidance notes

52. Several securities issuer service providers are likely to provide services to the securities issuer. Each will be a *supervised person*, with the securities issuer as their *customer*. Each will have their own *CDD* obligations pursuant to the *Money Laundering Order*.

53. Even where a securities issuer service provider is not providing investor-facing services and only provides services to the securities issuer, they should ensure when conducting their *CRA* (of their *customer* – the securities issuer) that they obtain sufficient information on the investors (e.g., *source of funds*) and *Beneficial owners and/or controllers* of the securities issuer. Rather than gathering this information themselves, in a low-risk scenario the securities issuer may be able to provide a list of its investors with holdings of 25% or more and *source of funds* information provided to the securities issuer by investors via subscription agreements/investor questionnaires (see also paragraph 135 below).

54. The first step for a *supervised person* is to determine the nature of their *customer* and determine the *customer's* potential *Beneficial owners and/or controllers*, any third parties on whose behalf the *customer* acts (and any third party's *Beneficial owners and/or controllers*) and others listed in Article 3(2) of the *Money Laundering Order*. It may not always be necessary to verify all of them.

55. The application of Article 3 of the *Money Laundering Order* differs depending on the legal form of the securities issuer. For the examples in the two tables below it is assumed that both the general partner and trustee are companies.

Application of Article 3 where the securities issuer service provider's *customer* is a:

Legal person, i.e., a company			
Customer	Third party	Owners/Investors of the securities issuer	*Governing body*
Company Article 3(2)(a), (aa) and (c) of the *Money Laundering Order.*	N/A.	Shareholder(s) (owns *customer*) Article 3(2)(c)(iii) of the *Money Laundering Order.*	Directors of company Re *customer.* Article 3(2)(aa), c(ii) and c(iii) of the *Money Laundering Order.*
Legal arrangement, i.e., a limited partnership/unit trust			
General partner/Trustee (company) Article 3(2)(a),(aa) and (c) of the *Money Laundering Order.*	Limited partnership/Unit trust Article 3(2)(b)(iii) of the *Money Laundering Order.*	Limited partner(s)/ Unit holder(s) (owns third party) Article 3(2)(b)(iii)(A), (B) and (C) of the *Money Laundering Order.* (Note: the requirements of Article 3(7) of the *Money Laundering Order*).	Directors/ Shareholders of general partner/ trustee › Re *customer* Article 3(2)(aa), c(ii) and c(iii) of the *Money Laundering Order.* › Re third party Article 3(2)(aa), (b)(iii)(A), (B) and (C) of the *Money Laundering Order.*

56. Once a *supervised person* fully understands the ownership and control structure of a *customer* the *supervised person* can determine the *beneficial owners and controllers* pursuant to the Three Tier Test and then apply the necessary *identification measures*.

57. The Three Tier Test is applied on a case-by-case basis and the table below indicates potential *Beneficial owners and/or controllers* in different scenarios where the ***supervised person* is a** securities issuer service provider, **and the securities issuer is a**:

Legal person, i.e., a company		
Customer	Third party	*Beneficial Owners and/or controllers*
Company. Article 3(2)(a), (aa) and (c) of the *Money Laundering Order.*	N/A.	Apply the Three Tier Test (see above) › Shareholder(s) Article 3(2)(c)(iii) of the *Money Laundering Order* - Potentially Tier 1 › Promoters/Instigators Article 3(c)(ii) of the *Money Laundering Order* - Potentially Tier 2 › Directors of Company - Potentially Tier 3 Article 3(2)(aa), (c)(ii) and (c)(iii) of the *Money Laundering Order.*
Legal arrangement, i.e., unit trust/limited partnership		
General partner for limited partnership/trustee for unit trust (company) Article 3(2)(a), (aa) and (c) of the *Money Laundering Order.*	Limited partnership/unit trust Article 3(2)(b)(iii) of the *Money Laundering Order.*	Apply the Three Tier Test to the *customer* and the third party: › *customer* – general partner/trustee Article 3(2)(aa) and (c) of the *Money Laundering Order.* › Third Party - limited partnership/trust Articles 3(2)(b) and 3(7) of the *Money Laundering Order.*

58. More detailed guidance on how to determine and identify *Beneficial owners and/or controllers* is contained in the following sections of *this Handbook*:

Entity	**Finding out identity**	**Obtaining evidence**
Limited partnership	4.3.3	4.3.4
Trust (not unit trust)	4.3.1	4.3.2
Company	4.5.1	4.5.2

13.3.3 Identification Measures - unit trusts

Securities issuers

Guidance notes

59. Unit trusts differ from traditional private trusts. For example, with a private family trust there is normally a settlor who not only establishes the trust but also provides the initial funds and ongoing funding to the trust. Beneficiaries may be expressly referred to or may form part of a class and may not have a vested right to the trust assets.

60. In a unit trust the promoter or instigator may fund the establishment of the unit trust and may fund the initial investment, thus being considered a settlor. While the individual investors are not considered to be settlors for the purposes of Article 3(7)(a) of the *Money Laundering Order*, each of the unit holders will be *customers* of the securities issuer (unit trust) investing their money into the unit trust. This may include the promoter as an investor.

61. Statutory requirements relating to *identification measures* that apply to unit trusts are set out at Article 3(7) of the *Money Laundering Order*.

13.3.4 Securities issuer service provider – passive investors

Securities issuers

Guidance notes

62. Identification of investors in a securities issuer will be approached differently by the securities issuer and the securities issuer service provider.

63. The securities issuer has an obligation to identify each of its investors, as they are the securities issuer's *customers*. This obligation exists regardless of whether they are passive investors who do not exercise control over the securities issuer.

64. The securities issuer service provider, however, has an obligation to identify the *Beneficial owners and/or controllers* of their *customer* (the securities issuer) and should apply the Three Tier Test to ascertain who the *Beneficial owners and/or controllers* are. Where ownership of a securities issuer is distributed widely, it may be that none of the investors control the securities issuer through their ownership. In such a case, these "passive" investors are not *Beneficial owners* at Tier 1 and, assuming they are not controllers via Tier 2 or 3, a securities issuer service provider need not apply *identification measures* to them.

65. It should be noted, however, that to demonstrate that sufficient information has been collected on *source of funds* for a *customer* relationship, it may still be necessary to consider the provenance of investors who have a **material interest** in a *customer*, but who do not also **exercise control**. The effect of this may still be to require information to be obtained on such passive investors (though it may not be necessary to also obtain evidence of identity).

66. For example, an investment advisor giving advice directly to a regulated fund with passive investors will still need to obtain *source of funds* information in relation to those investors to understand the *AML/CFT/CPF* risk posed by its *customer*.

67. The extent of *source of funds* information collected will be proportionate to the risks identified and determined on a case-by-case basis. In a lower risk relationship, *source of funds* information should be obtained for all passive investors with a holding of **25% or more**. Where there are no 25%+ holders, generic investor information on *source of funds* such as a generic profile could be obtained. In a higher risk relationship, more stringent measures should be applied. These measures should be determined on a case-by-case basis with reference to the *supervised person's CRA* of the relationship.

68. Similarly, to demonstrate that sufficient information has been collected to assess the *AML/CFT/CPF* risks posed by a *customer*, it may be necessary to consider the identity, nature, structure and location of investors who have a **material interest** in a *customer*, but who do not also **exercise control**. See sections 3.3.2 and 3.3.4 of *this Handbook* for further detail.

13.3.5 Securities issuer service providers - promoters

Securities issuers

Guidance notes

69. A *supervised person* may need to consider whether the promoter of a securities issuer is a *Beneficial owner and/or controller*. For example, the promoter/instigator of the securities issuer may have direct control by owning the *Governing body* (i.e., the general partner or the trustee) or by owning management shares of a securities issuer company.

70. In addition, a promoter may also be a *Beneficial owner and/or controller* where the board of a securities issuer does not exercise sufficient effective control. For example, a promoter may be the investment adviser/investment manager or may have a significant presence on the investment committee, which may indicate **control by other means** (see Tier 2 of the Three Tier Test).

13.3.6 Multiple layers

Overview

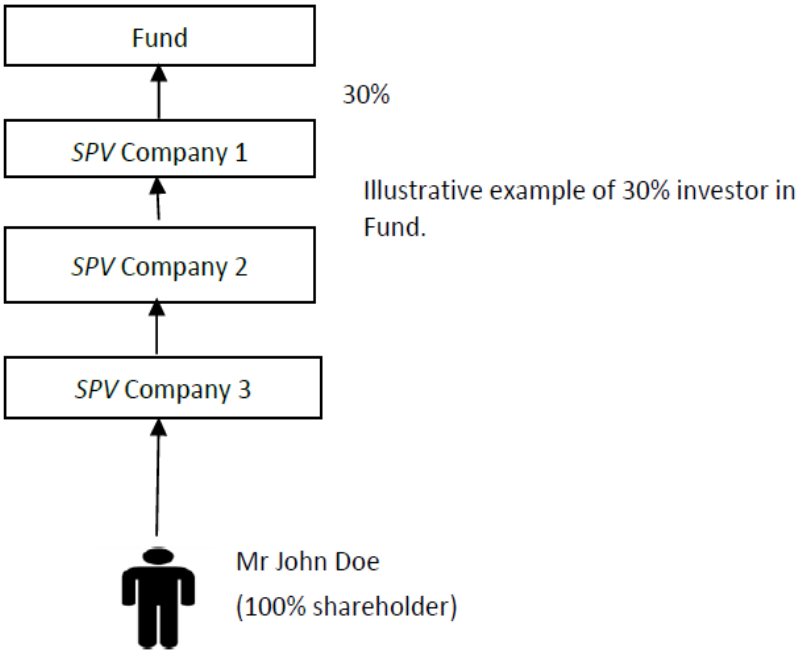
71. Securities issuers' structures are often complicated by ultimate *Beneficial owners* not entering into transactions directly and there may be multiple entities, such as holding companies, trusts, nominees, and intermediaries between the investment in the securities issuer and the individual who is the ultimate *Beneficial owner*. The more complex the structure, the more difficult it may be to determine the *Beneficial owner and/or controller* (see *Complex Customer Structures section 7.8)*

72. A *supervised person's* approach to a complex ownership and control structure will be informed by the risk rating allocated to that *customer*. However, as set out in section 4 of *this Handbook*, the following are always required to be identified:

- the *customer*;
- the ultimate Beneficial owners and/or controllers of the *customer* (the Three Tier Test can assist *supervised persons* in working out which persons fall within this category); and
- any third parties on whose behalf the *customer* acts.

Guidance notes

73. In the example below the securities issuer (in this case a fund) is the *supervised person*. The general rule is that you are trying to ascertain the ultimate individual(s) who control(s) the structure.



Customer

74. *SPV* company 1 is the *customer* of the fund.

75. The fund is obliged to find out the identity of its *customer* and obtain evidence of identity. *This Handbook* provides guidance on *identification measures* to be applied to a legal person that is a company:

- section 4.5.1 - Finding out the identity of a legal person that is a company, and
- section 4.5.2 - Obtaining evidence of identity of a legal person that is company.

Beneficial Owner and/or controller

76. *SPV* company 1 is a legal person, and the *supervised person* must understand the ownership and control structure of the *customer*. The fund is obliged to find out the identity and obtain evidence of identity of its *Beneficial owners and/or controllers*. The Three Tier Test is applied to ascertain who controls the *customer*:

- control via ownership; and
- control via other means; or
- control through positions held (if no-one at Tiers 1 and/or 2).

77. Understanding a *customer*'s ownership and control structure will allow a *supervised person* to determine the ultimate Beneficial owner and/or controller. Article 2(2) of the *Money Laundering Order* states "…. it is immaterial whether an individual's ultimate ownership or control is direct or indirect".

78. In this example the structure is in place for the purpose of facilitating the investment of John Doe and he is exercising effective control. Therefore, regardless of the holding companies, John Doe is the Beneficial owner and/or controller of the *customer*.

79. *This Handbook* provides guidance for individuals (in this example John Doe):

- section 4.2.2 of *this Handbook* - Finding out the identity of an individual;

- section 4.2.3 of *this Handbook* - Obtaining evidence of identity of an individual.

80. If none of the individuals with ownership interests **exercise control,** then they may not need to be identified (section 13.2.4 of *this Handbook* regarding passive investors).

Multi-layered structure

81. In the above scenario understanding the ownership and control structure of the *customer* is likely to require some effort, but it may not be necessary to obtain detailed identity information and evidence in relation to each entity in the structure.

82. Verification of identity may not be necessary in relation to *SPV* company 2 and *SPV* company 3 – they are not *customers* or *Beneficial owners and/or controllers* or third parties on whose behalf the *customer* is acting (see paragraph 72 above). The reason they are not controllers is because they are acting on the instructions of the **ultimate controller** Mr John Doe and are therefore merely links in the control chain.

83. Whilst obtaining evidence of identity may not be necessary, sufficient information will still need to be obtained in relation to these two entities to understand the wider ownership and control structure. The information required will depend on the complexity of the structure and the overall risk of the *customer* relationship. However, as a minimum for a low-risk *customer* the following should be obtained:

- name of the entity;
- evidence the entity exists;
- names of the directors;
- names of the shareholders or those with other interests;
- details of ownership and control of the entity (proportion of holdings, voting rights, decision-making authority, etc.).

13.3.7 Nominees/investment managers

Guidance notes

84. This section is supplemental to and should be read in conjunction with section 8.2 of *this Handbook* regarding *Designated relationships* and *pooled relationship*s.

85. There may be scenarios where the securities issuer's *customer* is representing other parties, for example as a nominee/investment manager. In this scenario the normal obligations apply, and the *supervised person* still has to identify:

- the *customer*;
- the ultimate Beneficial owner and/or controller of the *customer* (as per the Three Tier Test);
- any third parties for whom the *customer* acts.

86. If the *customer* is a company, then the *supervised person* would apply the guidance in paragraph 75 above.

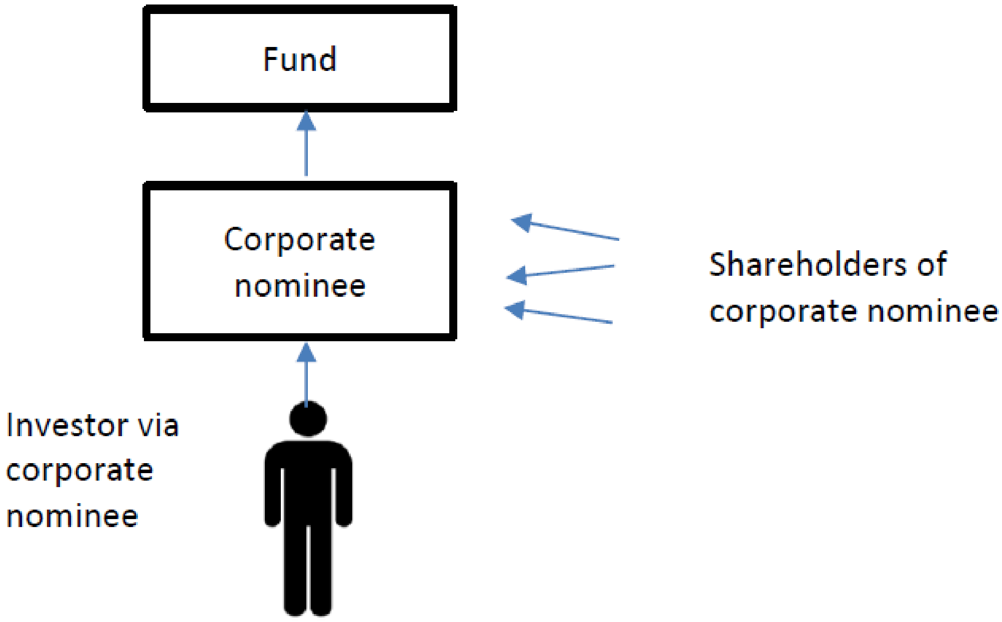
87. In the scenario below the securities issuer (in this case a Fund) is the *supervised person*, the corporate nominee is the *customer,* and the individual is the third party for whom the *customer* is acting.

88. The corporate nominee is the *customer,* and it will be necessary to identify its *Beneficial owners and/or controllers*. The Three Tier Test will need to be applied to determine the potential *Beneficial owners and/or controllers* of the corporate nominee. In this scenario it will also be necessary to identify the third party for whom the corporate nominee is acting and determine the *Beneficial ownership and/or control* of that third party as per Article 3(2)(b) of the *Money Laundering Order*.

Illustrative example of application of the Three Tier Test to

A corporate nominee - *(Article 3(2)(c)* of the *Money Laundering Order*		
No.	Control through ownership.	There are several owners and there is no majority shareholder.
No.	Control through other means.	There are no entities/persons that fall into this tier.
Yes.	Control through positions held.	The board of directors control the corporate nominee.

An individual whose interest is through the corporate nominee - Article 3(2)(b) of the *Money Laundering Order*		
Yes.	Control through ownership.	Here the principal is an individual.
No.	Control through other means.	Tier 1 applies so no further need to determine potential persons in other tiers.
No.	Control through positions held.	



89. The *supervised person* is required to identify and verify its *customer* – here the corporate nominee – as set out at paragraph 75 above. Control and ownership of the *customer* must be ascertained applying the Three Tier Test (paragraph 88 above).

90. The third party for whom the *customer* is acting must also be identified and verified. In the diagram above this will be the individual who is investing via the nominee. If the third party in the example above was not an individual, then its *Beneficial owners and/or controllers* would also need to be identified and verified.

13.3.8 Securities issuer service providers – residual assets

Securities issuers

Guidance notes

91. On some occasions when a securities issuer is wound up the securities issuer service provider may hold residual and/or illiquid assets of the securities issuer for the benefit of the investors. In this scenario care has to be taken and the following matters should be considered:

- Have the investors now become the securities issuer service provider's *customers*?
- Does the securities issuer service provider hold sufficient *CDD* on its *customers*? For example, the securities issuer service provider may have taken comfort from the *identification measures* applied **by the** securities issuer, but the securities issuer no longer exists;
- Has the securities issuer service provider updated its *CRA* and *BRA* to take into consideration its new role (regardless of whether the investors are its *customers*)?

13.4 Timing of *identification measures*

Securities issuers

Overview

92. This section is supplemental to and should be read in conjunction with sections 4.1 and 4.7 of *this Handbook*.

93. Article 13(4) of the *Money Laundering Order* provides a concession in relation to the timing of *identification measures*, permitting a delay in obtaining evidence in specific circumstances. However, **in no circumstances** can the obtaining of information be delayed.

Guidance notes

94. Delaying the obtaining of evidence is permitted in certain circumstances but should not be common or standard practice. It **should not** be common practice that verification is deferred until after the first close of a securities issuer. Where the provisions of Article 13(4) of the *Money Laundering Order* are relied upon to delay the obtaining of evidence of identity, additional measures are required, including the effective management of the associated risk through appropriate authorisation, monitoring, and reporting.

95. The obtaining of evidence of identity "as soon as reasonably practicable" should in most cases be a matter of days rather than weeks or months.

13.5 Failure to complete *identification measures*

Securities issuers

Overview

96. This section is supplemental to and should be read in conjunction with section 4.8 of *this Handbook*.

97. Under Article 14 of the *Money Laundering Order*, if a *supervised person* is unable to apply *identification measures* when required to do so then it must terminate that relationship and consider whether to make a *SAR* to the *FIU*.

98. This requirement may cause conflicts in the case of a *supervised person* that is a securities issuer where its *customer* is an investor and where:

- the relationship between the securities issuer and its investor is governed by other legislation or regulatory requirements, e.g., the *CIF(J) Law* and Code of Practice for Certified Funds; and
- the termination of a relationship with an investor may have a prejudicial effect on the interests of other investor, e.g., a closed-ended illiquid property fund.

Guidance notes

99. To address these potential issues, termination of a *business relationship* may be **delayed** until such time as compliance with Article 14 of the *Money Laundering Order* does not conflict with another statutory or regulatory requirement, and/or does not have any prejudicial effect on the interests of other *customers* (investors), so long as the risk of *money laundering,* the *financing of terrorism,* or the *financing of proliferation* is effectively managed.

13.6 Updating identification information

Securities issuers

100. This section is supplemental to and should be read in conjunction with sections 3.4 and 4.1 of *this Handbook*.

Guidance notes

101. The *BRA* will enable a *supervised person* to establish procedures to undertake reviews of its *customers* on a risk sensitive basis. In addition to the established pattern of reviews there will be “trigger events” when it may be appropriate to consider whether the identity information and evidence held on a *customer* is relevant and up to date. These should include (in addition to those circumstances set out in section 3.3 of *this Handbook*):

- receipt of significant additional funds to be invested where the delay between contributions is material (including drawdowns);
- when distributions are being made;
- economic merger of two securities issuers which results in the admission of new investors;

The guidance set out at section 3.4 of *this Handbook* regarding the taking on of a new book of business should also be considered, where relevant.

102. It may well be that when a *customer's* information and evidence of identity is reviewed upon a trigger event, the information and evidence previously obtained is sufficient and no further updated information is needed. This may be the case when, for example, a regularly scheduled review has recently been undertaken, and updated information has been received as a result.

13.7 Ongoing monitoring: scrutinising of transactions & activity

103. This section is supplemental to and should be read in conjunction with section 6 of *this Handbook*.

Guidance notes

104. The information about a *customer* obtained at the outset of the relationship as part of *identification measures* should allow a *supervised person* to monitor activity against an expected pattern of activity and transactions. For securities issuers this will include generic profiles of the expected target investors and the expected target investments. For example, if the securities issuer's prospectus/offer document indicates that it is going to invest in UK real estate and then invests in oil exploration and extraction businesses, this is not expected activity. Similarly, if the securities issuer is aiming for investment from European Banks and then receives investment from a *NPO* based in Sub-Saharan Africa, this would not be expected activity.

105. It is not sufficient for an administrator/manager who has been delegated the responsibility for monitoring the securities issuer to simply facilitate the transaction - they are also required to monitor each transaction to determine whether it is inconsistent, unusually complex/large, high risk or follows an unusual pattern. If a transaction does not match the expected profile, then the rationale for the transaction should be obtained and documented.

106. Expected activity may change over time if the target market or target investments change. This may also impact on the securities issuer's *BRA* and *CRAs* which may need to be updated.

13.8 Collation of *CDD*

Overview

107. Every securities issuer and securities issuer service provider are obliged to comply with the *CDD* requirements placed upon it. However, there may be statutory or contractual provisions operating so that, should one entity in a securities issuer structure undertake sufficient *CDD*, others in the structure may not need to duplicate certain aspects of *CDD* themselves.

108. The following sections of *this Handbook* deal with specific provisions regarding scenarios where a *supervised person* may not undertake all the *CDD* process themselves:

Exemptions from *identification measures*	› Section 8
Reliance on *obliged persons*	› Section 5
Outsourcing	› Section 2.4.4 › Section 5.1, paragraph 14

109. Where a *supervised person* **is not** undertaking aspects of *CDD*, including through the application of exemptions, it needs to:

- document who **is** doing so and on what basis; and
- ensure that the risks have been properly assessed, considered, and documented.

13.8.1 Exemptions from *identification measures*

Overview

110. This section is supplemental to and should be read in conjunction with section 7 of *this Handbook*.

111. An assessment as to whether exemptions from *identification measures* are appropriate for *customers* and/or in relation to third parties must be conducted and documented. When doing so the statutory prohibitions, stating where exemptions cannot be applied, must be carefully considered in each case:

Circumstances in which exemptions under Part 3A of the *Money Laundering Order* do not apply (Article 17A of the *Money Laundering Order*)	
Exemptions under Articles 17 B-D of the *Money Laundering Order*	**Exemptions under Article 18 of the *Money Laundering Order***
› the *supervised person* suspects *money laundering.*	› the *supervised person* suspects *money laundering.*
› the *supervised person* considers that there is a higher risk of *money laundering*, including the risk of *money laundering* if fail to apply appropriate *identification measures* or keep records.	› the *supervised person* considers that there is a higher risk of *money laundering.*
› the *customer* is resident in a country that is not compliant with the *FATF Recommendations.*	› the *customer* is resident in a country that is not compliant with the *FATF Recommendations.*
› the *customer* is a person in respect of whom Article 15(1)(c) of the *Money Laundering Order* applies [specified persons having a *relevant connection* to country/territory in relation to which *FATF* has called for *enhanced customer due diligence*].	› the *customer* is a person in respect of whom Article 15(1)(c) of the *Money Laundering Order* applies [specified persons having a *relevant connection* to country/territory in relation to which *FATF* has called *for enhanced customer due diligence*].
› the *customer* is a person in respect of whom Article 15B(1) of the *Money Laundering Order* applies [certain *cross border correspondent banking and other similar relationships* with a banking or similar relationship with an institution whose address for that purpose is outside Jersey].	

112. Exemptions from *identification measures* may only be applied in appropriate circumstances. Where specified, this will require an assessment of the risk of applying the exemption, in addition to a *CRA*.

Guidance notes

113. As noted at Section 8 of *this Handbook*, Articles 18 and 17B-D of the *Money Laundering Order* can be applied to the same *customer* relationship, as they apply to separate identification requirements.

114. Refer to the table set out at section 8.1.3, 8.2.2 and 0 of *this Handbook* for detail on which aspects of *CDD* must always be undertaken by the *supervised person*.

115. Article 18 of the *Money Laundering Order* applies only to the *customer* and does not extend to third parties. From a securities issuer service provider's perspective this means, for example, that Article 18 only applies to the general partner or the trustee and not to the limited partnerships or unit trust. Articles 17B-D of the *Money Laundering Order* **do apply** to third parties which would encompass the investors in a limited partnership or a unit trust.

116. Article 18(4)(b) of the *Money Laundering Order* refers to a *customer* that is a body corporate or *limited liability company* whose securities are listed on an *IOSCO* compliant exchange or on a *regulated market*. As part of the assessment whether simplified *CDD* may be applied, the *supervised person* should consider whether the exchange on which the securities are listed is an *IOSCO* compliant exchange or a *regulated market*. The fact that the exchange is listed in a product guide (e.g., Listed Fund Guide) or in an Order (e.g., the Collective Investment Funds (Unregulated Funds) (Jersey) Order 2008) does not necessarily mean it qualifies. Further guidance is provided on this point in section 0, and specifically, 8.3.4 of *this Handbook*.

13.8.2 Reliance on obliged persons

117. This section is supplemental to and should be read in conjunction with section 5 of *this Handbook*.

Guidance notes

118. Care should be taken when placing reliance on an administrator. An administrator may be acting in two capacities when undertaking *CDD*;

- for itself as securities issuer service provider and
- as a delegate on behalf of the securities issuer. In such a case, a *supervised person* seeking to rely on *CDD* undertaken by the administrator needs to be clear whether it is the administrator or the securities issuer that is the *obliged person.*

119. Set out below are some key questions for a *supervised person* to ask themselves:

- what *identification measures* do you need to apply?
- who are you intending to rely upon?
- what identification information and evidence has the *obliged person* obtained?
- does the information and evidence obtained by the *obliged person* being relied upon match your requirements?

120. Each securities issuer service provider will have its own risk appetite and its own *CRA* of the securities issuer and the risk ratings allocated by different securities issuer service providers may not be the same. Where a securities issuer service provider assesses the securities issuer as higher risk it may be insufficient to rely on information and evidence obtained by a securities issuer service provider rating the securities issuer as lower risk and additional information is likely to be required.

121. Importantly, chains of reliance are not permitted. A *supervised person* cannot rely on an *obliged person* who is in turn relying on someone else.

122. Reliance may be used where the securities issuer structure has higher *AML/CFT/CPF* risks, or the securities issuer structure and securities issuer service providers are unregulated (where the securities issuer service provider cannot apply exemptions from *identification measures*).

123. There are aspects of *CDD* that, in the absence of other provisions, the *supervised person* is required to undertake itself. These are set out in the table at section 5.1 of *this Handbook*.

13.8.3 Obtaining copy documentation from a *CD regulated TCSP*

Overview

124. This section is supplemental to and should be read in conjunction with sections 4.3.5 and 4.5.7 of *this Handbook*.

125. In certain circumstances, it may be appropriate to obtain information from a *CD regulated TCSP* to identify certain individuals.

126. It should be noted that such practice is restricted to a very narrow set of circumstances (e.g., only certain individuals and only certain documents) and is dependent on several conditions being met (e.g., a specific risk assessment is carried out and specific confirmations are obtained from the *TCSP*).

13.8.4 Outsourcing

Overview

127. This section is supplemental to and should be read in conjunction with sections 2.4.4 and 5 (paragraph 14) *of this Handbook*, along with the *JFSC's* Outsourcing policy.

128. Contractual arrangements may be put in place where another entity undertakes *CDD* for the *supervised person* as a delegate. This is likely to be the case where an administrator and/or manager is appointed to the securities issuer or where the *Governing body* of the securities issuer such as a trustee or general partner is a managed entity and reliant on a manager of a managed entity. The *supervised person* always remains responsible for fulfilling its statutory obligations regardless of the activities it outsources to delegates.

129. Procedures and processes must be put in place so that the delegating party retains oversight of the outsourced activities. The *supervised person* needs to be provided with sufficient information by the delegate to adequately review and monitor the outsourced activities.

Guidance notes

130. Outsourcing of specific functions to a securities issuer service provider may form part of the securities issuer service provider's service level agreement with the securities issuer. The *supervised person* would be expected to ensure that the terms are adequate to ensure a clear understanding of what activity the delegate is undertaking.

131. Given that the delegate carrying out the outsourced function is likely to have its own *CDD* obligations it will be important to distinguish between measures applied on behalf of the delegating party and measures applied for itself. This will ensure the respective (and potentially differing) obligations are met and will assist if the delegating party moves to another securities issuer service provider and wishes to take its information/documentation/records with it.

132. Section 2.4.4 of *this Handbook* provides a table of activities which may be outsourced but also states that *CDD* is always the responsibility of the *supervised person*.

133. Where *CDD* functions are outsourced, consideration will need to be given to the contractual arrangements between the securities issuer and its investors (*customers*), the securities issuer and its securities issuer service providers and any other entities. Below are some important matters to consider (this list is not exhaustive):

› which party has "ownership" of the investor information;

› permissions required from the investor for obtaining, holding and using the information for other purposes (data protection);

› the nature and scope of the obligations outsourced and provisions for monitoring, updating, retention and termination.

134. Where a securities issuer service provider assesses the *AML/CFT/CPF* risk regarding a securities issuer to be higher or the securities issuer/securities issuer service providers are not regulated, the application of exemptions from *identification measures* is prohibited. Therefore, a securities issuer service provider providing services to a securities issuer where it has no direct relationship with the investors may need to apply *identification measures* to the investors. This may be in relation to the control of the securities issuer or its *source of funds*. Rather than gathering this information themselves they will instead seek access to this information which will normally already have been provided to the securities issuer by investors via subscription agreements/investor questionnaires.

135. Note that specific provisions may be necessary in subscription agreements/investor questionnaires to enable the securities issuer to pass on information and evidence that it obtains to meet its own *AML/CFT/CPF obligations*, to assist securities issuer service providers (present and future) involved in the securities issuer/securities issuer structure to meet their own *AML/CFT/CPF obligations* (subject to any data protection requirements).

13.8.5 AMLSP

136. Section 15 of *this Handbook* provides guidance where an eligible *supervised person* appoints an *AMLSP* to fulfil its *AML/CFT/CPF obligations*. Where a securities issuer and their service providers are eligible, an *AMLSP* may be used. The section also provides guidance in certain circumstances where the securities issuer is a legal arrangement represented by its legal person *Governing body* and the legal person can use the *AMLSP* to provide services both to itself in its own capacity and in its capacity as *Governing body*, e.g., a Jersey private fund which is a limited partnership with an *SPV* general partner.

13.9 *Enhanced CDD measures* – non-Jersey investors

Overview

137. This section is supplemental to and should be read in conjunction with sections 7, 7.4 and 7.7 of *this Handbook*.

138. Securities issuers with overseas investors will need to undertake *enhanced CDD measures to* those investors (see Article 15 of the *Money Laundering Order*) as the investors will normally be:

› non-resident *customers*; and/or

› not physically present for identification purposes.

139. *Enhanced CDD measures* must be applied to address the risk associated with these types of *customers*. Sections 7.4 and 7.7 of *this Handbook* provide guidance on the same.

Guidance notes

140. A requirement to apply *enhanced CDD measures* does not automatically mean that the *customer* is higher risk. Some enhanced measures are required regardless of risk.

141. It may be possible for investor profiles/subscription agreements to address *enhanced CDD measures* requirements by obtaining additional information if the investor meets certain criteria. For example, a question might read “Are you Jersey resident? If the answer is no, provide the following additional information…”.

142. On some occasions the rationale for a non-Jersey investor looking to invest in Jersey may be determined without necessarily needing to ask the *customer* (e.g., it may be obvious if, say, the securities issuer is a Jersey securities issuer).

14 *WIRE TRANSFERS AND PREPAID CARDS*

14.1 Wire transfers

14.1.1 Overview of section

1. The *Wire Transfers Regulations* were brought into force on 13 June 2017, following the EU's enactment of the *EU Regulation* on 20 May 2015. It implements *FATF Recommendation* 16 and promotes an enhanced framework around the traceability of transfers of funds for the purpose of preventing, detecting and investigating *money laundering,* the *financing of terrorism,* or the *financing of proliferation* and other *financial crime*s.

2. The *EU Regulation* expanded the regulatory requirements with the following objectives:

- to prevent the abuse of fund transfers for *money laundering*, *terrorist financing* and other *financial crime* purposes;
- to detect such abuse should it occur;
- to support the implementation of restrictive measures; and
- to allow *supervised* authorities to access the information promptly.

3. In this section, any reference to a numbered Article, without further detail, is a reference to the Article so numbered inf the EU Regulation.

Statutory Requirements (paraphrased wording)

4. ***Regulation 2 of the Wire Transfers Regulations gives the EU Regulation full force and effect, subject to certain adaptations, exceptions and modifications as set out in its Schedule 1.***

5. *Under the Wire Transfer Regulations, the following definitions apply:*

6. *"money or value transfer service provider"* ***(MVTS)*** *means a person who provides a money or value transfer service within the meaning given in paragraph 5 in Part 2 of* Schedule 2 *of the Proceeds of Crime (Jersey) Law 1999.*

7. *"payment service provider" (**PSP**) means a person, being a person registered under the BB(J) Law, or who is a VASP or a MVTS, when:*

- *the person is carrying out payment services in or from within Jersey; or*
- *being a legal person established under Jersey law, the person is carrying out payment services in any part of the world other than in or from within Jersey.*

8. *"intermediary payment service provider" (**IPSP**) means a PSP that is neither that of the payer nor that of the payee and that participates in the execution of transfers of funds;*

9. *"payer" means a person that is the holder of an account held with a PSP that allows a transfer of funds or value from the account or, where there is no account, a person that places an order for a transfer of funds;*

10. *"payee" means a person that is the intended final recipient of transferred.*

11. *"virtual asset" has the meaning given in Part 1 of* Schedule 2 *to the law.*

12. *"virtual asset service provider"* **(VASP**) *has the meaning given in Part 4 of* Schedule 2 *to the law.*

13. Article 2*A(1)* of the Wire *Transfer* Regulations, *states that* Article 2 of the Wire Regulations shall not apply *(and hence the EU Regulations do not apply)* to transfers of virtual assets equivalent to less than EUR 1,000.00 if the payer and payee are both *VASPs*.

14. *D*espite any other stipulation under the EU Regulations*, Article 2A(2) of the* Wire Transfer Regulations *requires that if* a payment service provider considers that there is a higher risk of *money laundering* in respect of virtual assets *then it* must comply with Article 2 of the Wire Transfer Regulations *(and hence the EU Regulations)* irrespective of the amount transferred if:

- *the payer is a VASP and the payee is not a VASP; or*
- *the payer is not a VASP and the payee is a VASP.*

Guidance notes

15. The core requirement is that every wire transfer must be accompanied by specific information (**complete information**) about the payer and the payee, which should be collected and retained by payment service provider or intermediary payment institutions, unless special exemptions and derogations apply, including funds transfers between the British Islands (referred in this section as being the *UK*, Jersey, Guernsey, and the Isle of Man).

16. A PSP should establish for each transfer of funds whether it acts as the PSP of the payer, the payee or as an IPSP. This will determine what information must accompany a transfer of funds and the steps required to comply with the *Wire Transfer Regulations*.

17. The *Wire Transfer Regulations* also require PSPs to put in place effective procedures to detect transfers of funds that lack the required information about the payer and the payee, and to determine whether to execute, reject or suspend such transfers of funds.

18. In line with the Data Protection (Jersey) Law 2018, personal data obtained by PSPs should be used only for the purpose of preventing *money laundering*, *terrorist financing,* or *proliferation financing*. PSPs should ensure the confidentiality of such data.

19. Any record of information on the payer/payee should not be kept longer than is necessary for the purposes of preventing, detecting, and investigating *money laundering,* the *financing of terrorism,* or the *financing of proliferation*.

20. Outside the normal data collection PSPs are expected to record information on the payer or payee. However, *Article 2A* of the *Wire Transfer Regulations* gives *PSPs* an exemption for transfers worth less than a €1000.00 between VASPs.

21. This exemption falls away if either the payer or payee is not a VASP, and the payment is high risk for *money laundering*. As such, *PSPs* must apply the *EU Regulations* as adopted into law, as per Article 2 of the *Wire Transfer Regulations.*

22. The risk factors to be considered are as stated under section 3.3.4.1 of *this Handbook*, in the cases highlighted at sections 4.3 and 4.5 of *this Handbook*.

23. The JFSC will be issuing a Guidance Note detailing the requirements for proprietary, inter-entity, Jersey-to-Jersey and inter-group transfers. The Guidance Note will also provide a steer on the suggested approach to the transfer of funds to unregulated VASPs in foreign jurisdictions.

24. The JFSC acknowledges that the process of integrating these requirements into a business' practice may take time. Supervision teams would expect that VASPs take reasonable steps towards the implementation of a solution and subsequent compliance with these requirements.

14.1.2 Scope of the Wire Transfer Regulations

Overview

Statutory requirements (paraphrased wording)

25. *Under Article 1 the EU Regulation, the Wire Transfers Regulations shall apply to transfers of funds, in any currency, which are sent or received by PSP or IPSP established in Jersey. These apply to credit transfers, direct debits, money remittances and transfers carried out using a payment card, an electronic money instrument, or a mobile phone, or any other digital or IT prepaid or post-paid device with similar characteristics, irrespective of whether the payer and the payee are the same person and irrespective of whether the PSP of the payer and that of the payee are one and the same. For British Islands-based PSPs, it includes, but is not necessarily limited to, international payment transfers made via SWIFT, including various Euro payment systems, and domestic transfers via CHAPS and BACS.*

26. *Article 2(2) provides the reference to exclusions from the scope of the Wire Transfer Regulations.*

27. *The Wire Transfer Regulations shall not apply to transfers of funds that represent a low risk of money laundering or the financing of terrorism under Article2(4), such as:*

- *transfers of funds, that involve the payer withdrawing cash from the payer's own payment account;*
- *transfers of funds to a public authority as payment for taxes, fines or other levies within the British Islands;*
- *transfers of funds where both the payer and the payee are PSPs acting on their own behalf;*
- *transfers of funds carried out through cheque images exchanges, including truncated cheques.*

28. *By way of exception, under Article 2(3), the EU Regulation shall not apply to transfers of funds carried out using payment cards, electronic money instruments, mobile phones or other digital or information technology (IT) prepaid or post-paid devices with similar characteristics, where the following conditions are met:*

a) *that card, instrument or device is used exclusively to pay for goods or services; and*

b) *the number of the card, instrument or device accompanies all transfers flowing from the transaction.*

29. *By way of derogation, under Article 2(5) the EU Regulation, the Wire Transfer Regulations shall not apply to transfers of funds within the British Islands to a payee's payment account permitting payment exclusively for the provision of goods and services where all the following conditions are met:*

a) *the PSP of the payee is subject to the requirements of the Money Laundering Order or the Terrorism Law or is subject to equivalent requirements under enactments of the UK, Guernsey or the Isle of Man;*

b) *the PSP of the payee is able to trace back, through the payee, by means of a unique transaction identifier, the transfer of funds from the person who has an agreement with the payee for the provision of goods or services;*

c) *the amount of the transfer of funds does not exceed €1,000.*

Guidance notes

30. A *supervised person* should have in place *systems and controls* (including *policies and procedures*) to ensure the conditions for the exemptions and derogations are met.

31. PSPs and IPSPs may demonstrate compliance with the *Wire Transfer Regulations* if they have in place relevant *systems and controls* (including *policies and procedures*) which set out clearly:

- which criteria they use to determine whether or not their services and payment instruments fall under the scope of the *Wire Transfer Regulations*
- which of their services and payment instruments fall within the scope of the *Wire Transfer Regulations* and which do not, and
- which information relating to transfers of funds is required to be recorded, how this information should be recorded, and where.

32. PSPs and IPSPs may demonstrate their compliance with the application of the exemption under Article 2(3) of the *EU Regulation* when they have procedures for identifying and documenting:

- that transfers by card, instrument or device are for goods or services, where the exemption applies, as opposed to person-to-person transfers and
- that their *systems and controls* ensure that the number of the card, instrument, or digital device, for example, the Primary Account Number (PAN), is provided in a way that allows the transfer to be traced back to the payer.

14.1.3 Outgoing transfers – obligations upon the PSP of the payer

14.1.3.1 Transfers for non-account holders

Statutory requirements (paraphrased wording)

33. Under Article 4(3) EU Regulation, the PSP of the payer shall ensure that transfers of funds are accompanied by the following complete information on the payer and the payee:

a) the name of the payer;

b) unique transaction identifier (which can trace a transaction back to the payer);

c) one of either the 'payer's address, official personal document number, customer identification number or date and place of birth;

d) the name of the payee; and

e) a unique transaction identifier (which can trace a transaction back to the payee).

34. These requirements apply to all types of transfers outside the British Islands and exceeding €1,000, whether those transfers are carried out in a single transaction or in several transactions which appear to be linked.

35. The 'unique transaction identifier' is defined as a combination of letters, numbers or symbols determined by the PSP, in accordance with the protocols of the payment and settlement systems or messaging systems used for the transfer of funds, which permits the traceability of the transaction back to the payer and the payee.

36. The following derogation applies, allowing for a reduced information to be provided:

- *Under Article 5 of the EU Regulation, where all of the PSPs involved in the payment chain are established in the British Islands, the transfer shall include at least the unique transaction identifier (which can trace a transaction back to the payer and payee) for the payer and the payee. If further information is requested by the PSP of the payee or the Intermediary PSP, such information shall be provided within three working days of the receipt of a request for such information;*
- *Under Article 6, where PSP of the EU Regulation of the payee is established outside the British Islands, transfers of funds not exceeding €1,000 shall be accompanied by at least: the names of the payer and the payee and the unique transaction identifier.*

Note: For transfers of funds not exceeding € 1,000 the PSP of the payer need not verify the information on the payer unless the funds to be transferred have been received in cash or in anonymous electronic money, or the PSP has reasonable grounds for suspecting money laundering or the financing of terrorism.

14.1.3.2 Transfers for Account holders

Statutory requirements (paraphrased wording)

37. *Under Article 4(1) and 4(2), where a transfer of funds is made from or to an account, the PSP of the payer shall ensure that transfers of funds are accompanied by the following complete information:*

   a) *the name of the payer;*
   b) *the payer's payment account number; and*
   c) *one of either the payer's address, official personal document number, customer identification number or date and place of birth;*
   d) *the name of the payee; and*
   e) *the payee's payment account number*

38. *These requirements apply to all types of transfers outside the British Islands and exceeding €1,000, whether those transfers are carried out in a single transaction or in several transactions which appear to be linked.*

39. *Under Article 5 and 6 of the EU Regulations the following derogation from the requirements of Article 4 apply:*

- *where all of the PSPs involved in a transfer are established in the British Islands, Article 5 of the Regulation requires that the transfer includes a payment account number of the payer and the payee. The account number could be but is not required to be, expressed as the IBAN. If further information (for example, the name and address of the payer) is requested by the PSP of the payee or the IPSP, such information shall be provided by the PSP within three working days;*
- *under Article 6, where PSP of the payee is established outside the British Islands, transfers of funds not exceeding €1,000 that do not appear to be linked to other transfers of funds which, together with the transfer in question, exceed €1 000, shall be accompanied by at least: the names of the payer and the payee and the payment account numbers of the payer and of the payee.*

Note: For transfers of funds not exceeding € 1,000 the PSP of the payer need not verify the information on the payer unless the funds to be transferred have been received in cash or in anonymous electronic money, or the PSP has reasonable grounds for suspecting money laundering or the financing of terrorism.

AML/CFT/CPF Codes of Practice

[COP125] In the case of a payer that is a company, a wire transfer must be accompanied by an address at which the company's business is conducted, or at which it may be contacted. In the case of a payer that is a trustee, a wire transfer must be accompanied by the address of the trustee.

Guidance notes

40. Linked transactions are defined as at least those transactions that are sent from the same payment account, or from the same payer to the same payee within a short timeframe, for example, within six months. *PSPs* and *IPSPs* may demonstrate that they are able to detect transfers of funds that appear to be linked where they provide, in their *policies and procedures*, examples of scenarios where transfers are found to be linked which are relevant to their type of business.

41. The exemptions for transfers within the British Islands arises from expediency, not principle, in order to accommodate transfers by domestic systems like BACS which are currently unable to include complete information. Accordingly, where the system used for a transfer within the British Islands has the functionality to carry complete information, it is considered a good practice to include it and thereby reduce the likely incidence of inbound requests from payee PSPs for complete information.

42. The verification requirement set out in the *Wire Transfer Regulations* will be met for an account holding *customer* of a PSP where the payer's identity has already been verified by *CDD measures* and is stored, in accordance with the *Money Laundering Order*.

43. To meet the technical limitations and to manage cases with multiple account holders and different addresses, the PSP of the payer may demonstrate compliance with the *Wire Transfer Regulations* by documenting the priority given to the payer's information in line with law enforcement purposes to trace the payer and for sanctions screening. For example, by de-prioritising titles and full middle names, whilst prioritising the initial of the given name and the full family name and at least the country and the city of address; or for joint accounts holders to provide both names, giving priority to family name over given names.

14.1.3.3 Batch Files – payments either inside or outside of British Islands

Statutory requirements (paraphrased wording)

44. *Under Article 6(1), transfers of funds from a single payer to several payees that are to be sent in batch files containing individual transfers shall carry only the payment account number or the unique transaction identifier of the payer, as well as complete information on the payee, provided that the batch file contains complete information on the payer that is verified for accuracy and complete information on the payee that is fully traceable.*

45. *Where the transfer is at or below the €1,000 threshold it need only include:*

(a) the names of the payer and or payee; and

(b) the payment account numbers of the payer and the payee or a unique transaction identifier if there is no payment account for one or both parties.

14.1.4 Incoming Transfers - Obligation on the PSP of the payee and IPSP

Overview

46. Under the Wire Transfer Regulations, the PSPs of the payee and IPSPs are required to implement a targeted and proportionate risk-based approach to the monitoring of incoming fund transfers. The PSP of the payer holds responsibility for communicating all mandatory wire transfer information, which must be transmitted in the designated data fields of the payment message scheme.

47. If the required information on the payer or the payee has been provided only in part (incomplete information) or has not been provided (missing information), there is an increased threat of *money laundering* or *terrorist financing* presented by anonymous transfers.

48. To address the potential risk presented by such transfers, PSPs of the payee should put in place the following measures, ensuring they are commensurate with and proportionate to the *money laundering* and *terrorist financing* risks to which the PSP or IPSP are exposed:

- effective *systems and controls* to detect transfers of funds that lack required information; and
- risk-based *policies and procedures* to determine whether to execute, reject or suspend a transfer of funds that lacks the required information.

49. Effective *policies and procedures* should be set up in a way that reflects the adoption of a risk-based approach and should clearly document the following aspects:

- which information relating to transfers of funds has to be recorded, how this information should be recorded, and where it is stored;
- which transfers of funds have to be monitored in real time and which transfers of funds can be monitored on an *ex-post* basis, and why;
- the obligations of members of staff where they detect missing or incomplete information and the processes they should follow.

50. PSPs of the payee should document which high-risk factors or combination of high-risk factors are to be considered when determining the risk-based approach, for example:

- residual risks (risk posed by the types of *customers*, products, services, and delivery channels);
- country risks (association with high-risk jurisdictions or relevant sanctions regimes);
- unusual value and volume of transactions (compared to their particular business model);
- a negative *AML/CFT/CPF* compliance record on the part of the PSP of the payer or the prior PSP in the payment chain.

51. PSPs of the payee and IPSPs should implement three methods of wire transfer monitoring: real-time monitoring, post-event monitoring, and random post-event sampling. It should be determined and documented which high-risk factors (or combinations of high-risk factors) will always trigger real-time monitoring, and which will trigger a targeted ex-post review. In cases where ex-post monitoring identifies concerns, subsequent transfers of funds should always be monitored in real time.

52. In addition to real-time and targeted ex-post monitoring, PSPs of the payee and IPSPs should regularly perform ex-post reviews on a random sample taken from all processed transfers of funds.

14.1.4.1 Admissible characters or input and missing information checks

Statutory requirements (paraphrased wording)

53. *Under Article 7(1) and Article 11(1), the PSP of the payee and the IPSP respectively shall implement effective procedures to detect whether the fields relating to the information on the payer and the payee in the messaging or payment and settlement system used to effect the transfer of funds have been filled in using characters or inputs admissible in accordance with the conventions of that system.*

54. *Under Article 7(2) and Article 11(2), the PSP of the payee and the IPSP shall implement effective procedures, including, where appropriate, ex-post monitoring or real-time monitoring, to detect whether the payer or payee information listed in those articles is missing.*

AML/CFT/CPF Codes of Practice

[COP126] A PSP of the payee must subject incoming payment traffic to an appropriate level of post-event risk-based sampling to detect non-compliant transfers.

Guidance notes

55. PSPs of the payee and IPSPs may demonstrate compliance with the *Wire Transfer Regulations* by conducting and documenting a risk assessment that covers their payment activities, taking into account the overall volume and jurisdictions of funds transfers and the roles of all bodies involved.

56. PSPs of the payee and IPSPs may demonstrate compliance with the obligation to detect inadmissible characters and inputs if their system's validation rules adopt certain controlling functions, for example, the automatic prevention of sending/receiving of payments/value with inadmissible characters or inputs.

57. Other specific measures may be considered for a "meaningful character check". For example, in some cases the payer and payee information fields may include incorrect or meaningless information which does not make sense, even if this information has been provided using characters or inputs in accordance with the conventions of the messaging or payment and settlement system, for example, "our client", 'my *customer*'', etc. A *supervised person* may identify these issues by undertaking sample testing, maintaining a list of commonly found meaningless terms and keeping it up to date.

58. In addition to real-time and targeted ex-post monitoring, PSPs of the payee and IPSPs may demonstrate an appropriate level of *systems and controls* where they perform ex-post reviews on a random sample taken from all processed transfers of funds.

59. PSPs of the payee and IPSPs may also wish to consider other specific measures, e.g., checking, at the point of payment delivery, that payer information is compliant and meaningful on all transfers that are collected in cash by payees on a "pay on application and identification" basis.

60. PSPs of the payee and IPSPs may draw on existing *policies and procedures* if they are considered sufficient to meet their obligations under the *Wire Transfer Regulations*, as long as those *policies and procedures* are subject to periodic reviews and updates, and training is provided to all relevant members of staff, including persons responsible for processing transfers of funds.

14.1.5 Managing transfers of funds with missing information or inadmissible characters or inputs

Statutory requirements (paraphrased wording)

61. *Under Article 8(1) and Article 12(1), the PSP of the payee and the IPSP shall implement effective risk-based procedures – including the measure referred to in Article 3(5) of the Money Laundering Order – for determining whether to execute, reject or suspend a transfer of funds lacking the required complete payer and payee information and for taking the appropriate follow-up action.*

62. *Under Article 8(2) and Article 12(2), the PSP of the payee and the IPSP should consider the most appropriate course of action on a risk-sensitive basis, which may initially include the issuing of warnings and setting of deadlines. Where the requested information is not provided by the set deadline, the PSP or IPSP should, in line with its risk-based policies and procedures:*

- *a) decide whether to execute or reject the transfer;*
- *b) consider whether or not the prior PSP in the payment chain's failure to supply the required information gives rise to suspicion; and*
- *c) consider the future treatment of the prior PSP in the payment chain for AML/CFT compliance purposes e.g. rejecting any future transfers of funds from that PSP, or restricting or terminating its business relationship with that PSP.*

63. *Under Article 9, separate from the decision whether to execute, suspend or reject a transaction, missing or incomplete information must be considered as a factor when assessing whether a transfer of funds, or any related transaction, is suspicious and whether a disclosure is to be made under Article 34D(4) of the Proceeds of Crime Law, Articles 21(2) of the Money Laundering Order or Article 21(4) of the Terrorism Law.*

Guidance notes

64. To determine whether to reject, suspend or execute a transfer of funds in compliance with Articles 8 and 12, PSPs of the payee and IPSPs may consider the *money laundering*, *terrorist financing*, or *proliferation financing* risks associated with that transfer of funds and document it, for example:

- › what *money laundering*, *terrorist financing,* or *proliferation financing* concerns the type of missing information gives rise to; and
- › what high-risk indicators have been identified that may suggest that the transaction presents a high *money laundering*, *terrorist financing,* or *proliferation financing* risk or gives rise to suspicion of *money laundering*, *terrorist financing,* or *proliferation financing*.

65. PSPs of the payee and IPSPs may demonstrate implementation of effective risk-based *policies and procedures* by documenting and recording all of their actions and reasons for their actions or inaction, including:

- › making a decision on rejecting the transfer and informing the prior PSP in the payment chain of the reason for the rejection;
- › making a decision on execution of the transfer and sending of a request for information, before or after crediting the payee's payment account or making the funds available to the payee;

- all appropriate follow-up steps taken to obtain the response, including the issuing of warnings and setting of deadlines, before either rejecting any future transfers of funds from that prior PSP or restricting or terminating its *business relationship* with that prior PSP.

14.1.5.1 Failure to provide information

66. *Under Article 8(2) and Article 12(2) should the PSP of the payer repeatedly fail to provide the required information on the payer or the payee, even after warnings and deadlines, the PSP of the payee or IPSP shall take further steps by:*

- *either rejecting any future transfers of funds from that PSP; or*
- *restricting or terminating its business relationship with that PSP.*

67. *The PSP of the payee or IPSP shall report that failure, and the steps taken, to the JFSC.*

Guidance notes

68. A range of criteria may be used in order to assess whether a PSP of the payer or IPSP is 'repeatedly failing' to provide information, for example:

- the percentage of transfers with missing information sent by a specific PSP or IPSP within a certain timeframe;
- the percentage of follow-up requests that were left unanswered or were not adequately answered by a certain deadline;
- the level of cooperation of the requested PSP or IPSP relating to previous requests for missing information;
- the type of information which is missing.

69. The report to the *JFSC* should be completed without undue delay and contain the following information as set out in the *JFSC* form at **Appendix E1** of *this Handbook*:

- the name of the PSP of the payer or IPSP identified as repeatedly failing to provide the required information;
- the country in which the PSP of the payer or IPSP is authorised;
- the nature of the breach, including:
  - the frequency of transfers of funds with missing information;
  - the period of time during which the breaches were identified; and
  - any reasons the PSP of the payer or IPSP may have given to justify their repeated failure to provide the required information.
- details of the steps the reporting PSP of the payer or IPSP has taken, including the issuing of warnings or deadlines up until the decision to restrict or terminate the relationship was made.

70. The obligation to report applies only to circumstances where information requests are not fulfilled and the PSP of the payee or IPSP invokes measures which restrict or terminate the *business relationship* with the PSP of the payer. The reporting requirement does not apply where a request for information is fulfilled by the PSP of the payer.

14.1.5.2 Additional obligations on IPSPs

Statutory requirements (paraphrased wording)

71. *Under Article 10, the IPSP shall ensure that all the information received on the payer and the payee that accompanies a transfer of funds is retained with the transfer.*

Guidance notes

72. IPSPs should satisfy themselves that their *systems and controls* enable them to comply with the requirement that all information on the payer and the payee that accompanies a transfer of funds is retained with that transfer. As part of this, IPSPs should satisfy themselves of their system's ability to convert information into a different format without error or omission.

14.1.6 Reporting of breaches

Statutory requirements (paraphrased wording)

73. *Under Article 21(1), PSPs shall notify the JFSC of any breaches of the Wire Transfers Regulations.*

74. *Article 21(2) requires PSPs to establish appropriate internal procedures for their employees, or persons in a comparable position, to report breaches internally through a secure, independent, specific and anonymous channel, proportionate to the nature and size of the PSP.*

75. *Under Regulation 3 of the Wire Transfers Regulations, a relevant person who contravenes any requirement of Article 21(2), shall be guilty of an offence and liable to imprisonment for a term of 2 years and to a fine. This applies to all PSPs and IPSPs, irrespective of the capacity within which the PSP or IPSP is acting.*

Guidance notes

76. A *supervised person* should ensure that any breach of the *Wire Transfer Regulations* is promptly reported to the *JFSC.*

77. The report to the *JFSC* should be completed without undue delay and contain the following information as set out in the form at Appendix E2 of *this Handbook*:

› the specific provision in the *Wire Transfer Regulations* which has been breached;

› the nature of the breach, including its cause;

› the date the breach was identified by the PSP; and

› where possible, a summary of the measures taken by the PSP in relation to the breach and any subsequent changes to its *systems and controls* (including *policies and procedures*) to mitigate against a recurrence.

78. A *supervised person* should establish *policies and procedures* for the internal reporting of breaches of the *Wire Transfer Regulations* and maintain a record of those breaches and action taken, ensuring sufficient confidentiality and protection for *employees* who report breaches committed within the *supervised person*.

14.1.7 Information, data protection and record retention

Statutory requirements (paraphrased wording)

79. *Under Regulation 3 of the Wire Transfers Regulations, a relevant person who contravenes any requirement of Articles 14, 15(2) or (3), or 16 of the EU Regulation shall be guilty of an offence and liable to imprisonment for a term of 2 years and to a fine. This applies to all PSPs and IPSPs, irrespective of the capacity within which the PSP or IPSP is acting.*

80. *Under Article 14 of the EU Regulation, a relevant person shall respond fully and provide without delay all requested information concerning wire transfers to Jersey authorities responsible for preventing and combating money laundering or terrorist financing.*

81. *Under Article 15(2) of the EU Regulation, personal data shall be processed by PSPs only for the purposes of the prevention of money laundering or terrorist financing and shall not be further processed in a way that is incompatible with those purposes. The processing of personal data for commercial purposes shall be prohibited.*

82. *Under Article 15(3) of the EU Regulation, PSPs shall provide new customers with the information required pursuant to the Data Protection (Jersey) Law 2018 before establishing a business relationship or carrying out an occasional transaction (i.e. a one-off transaction). That information shall, in particular, include a general notice concerning the legal obligations of PSPs under the EU Regulation when processing personal data for the purposes of the prevention of money laundering or the financing of terrorism.*

83. *Article 16 of the EU Regulation requires that information on the payer and the payee shall not be retained for longer than is strictly necessary. PSPs of the payer and of the payee shall retain records of the information referred to in Articles 4 to 7 for a period of six years.*

Guidance notes

84. The "authorities responsible for preventing and combating *money laundering* or *terrorist financing*" described in Article 14 of the *EU Regulations* should be understood in Jersey to be the *JFSC* and the States of Jersey Police, including the *FIU*.

14.1.8 Offences and criminal liability

Statutory requirements (paraphrased wording)

85. *Under Regulation 3 of the Wire Transfers Regulations, a relevant person, whether acting in the capacity of PSP of the payer, PSP of the payee or an IPSP, who contravenes any requirement of the specific provisions of the EU Regulations, which have effect in Jersey by virtue of Regulation 2, shall be guilty of an offence and liable to imprisonment for a term of 2 years, and to a fine as follows:*

- *PSP of the payer - Articles 4, 5, 6 (see section 11.3 Outgoing Transfers - Obligations upon the PSP of the Payer);*
- *PSP of the payee - Articles 7, 8, 9 (see section 11.4 Incoming Transfers - Obligations upon the PSP of the payee and IPSP);*
- *IPSP - Articles 10, 11, 12 (see section 11.4 Incoming Transfers - Obligation upon the PSP of the payee and IPSP).*

86. *In deciding whether a person has committed an offence under the Wire Transfers Regulations, the court shall take into account whether the person followed any relevant guidance that applies to the person, and which was at the time issued, adopted or approved by the JFSC under any other enactment.*

87. *A person shall not be guilty of an offence under the Wire Transfers Regulations if they took all reasonable steps, and exercised all due diligence, to avoid committing the offence.*

88. *Under Regulation 4(1) of the Wire Transfers Regulations, if an offence under these Regulations committed by a limited liability partnership, a separate limited partnership, any other partnership having separate legal personality or a body corporate is proved to have been committed with the consent or connivance of:*

> *(a) a person who is a partner of the partnership, or a director, manager, secretary or other similar officers of the body corporate; or*
>
> *(b) any person purporting to act in any such capacity;*
>
> *the person is also guilty of the offence and liable in the same manner as the partnership or body corporate to the penalty provided for that offence.*

89. *Under Regulation 4(2) of the Wire Transfers Regulations, if the affairs of a body corporate are managed by its members, paragraph (1) applies in relation to acts and defaults of a member in connection with the member's functions of management as if they were a director of the body corporate.*

14.2 Prepaid cards

Overview

90. This section helps *supervised persons* issuing prepaid cards in Jersey (**issuers**), whether directly or indirectly through an agent or a distributor. It covers:

- what electronic money is and the features of prepaid cards;
- the various operators involved in a prepaid card programme;
- examples of risk factors inherently associated with prepaid cards;
- examples of how prepaid cards have been used in Jersey by *money launderers;* and
- the relevant regulatory and supervisory framework in place in Jersey in respect of the provision of prepaid cards.

14.2.1 Electronic money

Overview

91. Electronic money is defined at paragraph 5(d)(15) of the Schedule to the *Wire Transfers Regulations* as "electronically (including magnetically) stored monetary value, as represented by a claim on the issuer, which is issued on receipt of funds for the purpose of making a payment transaction, and which is accepted by a person other than the issuer of the electronic money".

92. Examples of electronic money products and services include online payment services, card-based products (including prepaid cards), vouchers and mobile payment services.

93. Monetary value will be stored in an **online account** or held on a **stored-value card** (where the value is stored on a microchip embedded in the card). Both may be reloadable or non-reloadable. A **reloadable** account or stored-value card can be recharged after the initial funds have been loaded, usually for an unlimited number of times. A **non-reloadable** account or stored-value card can be charged only once and does not permit any other funds to be added.

94. Electronic money which is card-based uses the card for authentication to permit a *customer* to access their funds.

95. Where electronic money is not used it can instead be redeemed. **Redemption** is a process whereby a *customer* presents electronic money to the issuer and receives money in exchange at par value. Redemption should not be confused with the spending of electronic money when a prepaid card is used for purchase of goods or services from merchants.

96. Card-based electronic money may be used in an open or closed loop system. In an **open loop system** card may be used to purchase goods and services from any merchant or withdraw cash at *ATMs* operated by any merchant that is participating in the payment network. These cards provide access to the global *ATM* and payment network through the logo that the card is branded with (e.g., VISA, MasterCard and American Express). In a **closed loop system**, cards may be used only to purchase goods and services from a single merchant or a limited, closed network of merchants (e.g., gift cards, gift vouchers and gift certificates). These cards typically do not provide access to the global *ATM* network, cannot be recharged and have no "cash back" function.

14.2.2 What is a prepaid card?

Overview

97. Prepaid cards are a type of electronic money. The *FATF* has classified such cards as a type of *NPPS*. These are new and innovative payment products and services that offer an alternative to traditional financial services. Other types of *NPPS* include mobile payment services and internet-based payment services – these are not covered by this section.

98. Prepaid cards provide the holder with an authenticated access to pre-loaded funds. These funds can be held in an online account or on a stored-value card.

99. Prepaid cards can be utilised for a range of purposes, including transactions in other countries or territories. Some cards can be funded by cash or other electronic payment instruments and can be used for online shopping or to receive "cash back". Newer prepaid card features that are becoming increasingly common include making onward transfers of money from a prepaid card account to other accounts (known as person-to-person transfers) and setting up standing orders.

100. Prepaid cards are a retail product and are mostly used for making small value payments. Despite this, the range of functions which prepaid cards currently offer can make them attractive to criminals.

14.2.3 Who is involved in a prepaid card programme?

Overview

101. Several operators are normally involved in a prepaid card programme. These include:

Operator	Description
acquirer	The person which maintains the relationship with the retailer, provides the infrastructure needed for accepting a card payment (e.g., access to the point of sale (**POS**) terminal or the payment services supporting an e-commerce website) and normally operates the account in which the proceeds of the sale transaction are deposited.
distributor/ retailer	The person that sells, provides, or arranges for the sale of, prepaid cards on behalf of the issuer to *customers*. Distributors may also offer a separate range of services to these *customers*.
payment network operator	The person that provides the technical platform to perform transactions with the card at *ATMs* or points of sale at merchants.
issuer	The person that issues prepaid cards and against which the *customer* has a claim for redemption or withdrawal of funds.
programme manager	The person responsible for establishing and managing the prepaid card programme in cooperation with a bank or electronic money institution. The programme manager usually markets the prepaid cards and establishes relationships with banks and distributors or *customers*, and in many cases provides the data processing capability. Some prepaid card issuers manage their card programmes themselves (i.e., without using programme managers).
agent	For the purposes of this section of *the Handbook*, the agent is any person that issues prepaid cards on behalf of the issuer (the principal), whether by contract with, or under the direction of, the principal.

102. Article 1 of the *EU Directive* stipulates that the activity of issuing electronic money falls within its scope. Categories of electronic money issuers include:

› credit institutions;

› electronic money institutions (defined in Article 2 of the *EU Directive* as a legal person that has been granted authorisation to issue electronic money); and

› post office giro institutions.

103. An issuer will be considered to carry on a *supervised business* in or from within Jersey where it does so through a physical presence on the island or through a Jersey-based agent.

14.2.4 Risks associated with prepaid cards

Overview

104. The *FATF* issued a guidance paper in June 2013 regarding the application of a risk-based approach towards prepaid cards, mobile payments and internet-based payment services. This paper highlights the importance of taking a more enhanced and focused approach in areas where there are higher risks.

105. Whilst prepaid cards do not automatically present a higher risk of *money laundering*, *terrorist financing,* or *proliferation financing*, issuers will need to consider the specific risk factors of each card issued and determine its risk assessment based on the same. The risk of a prepaid card being misused will also depend on the product design and use and the effectiveness of *systems and controls* (including *policies and procedures*). Issuers are expected to exercise greater caution and **apply *enhanced CDD measures*** in instances where there is a **greater** *money laundering, financing of terrorism,* or *financing of proliferation* **risk** or where a product is designed and used in a way that is similar to a bank account.

106. The risk assessment of a prepaid card issuer will need to cover all relevant risk factors (e.g., *customer* profile, product design and functionalities, geographical location of main card funding and card spending activities).

Guidance notes

107. Prepaid cards are mostly used for making small value payments and transactions. They leave an audit trail in the system, unlike cash transactions. However, if certain risk factors are not adequately or effectively managed and mitigated, prepaid cards can become attractive or susceptible to *money launderers*, *terrorist financiers* or *proliferation financiers* of weapons of mass destruction.

108. The risk factors listed below do not constitute an exhaustive list and should not be considered in isolation. An accumulation of multiple risk factors will increase the overall risk level – such an accumulation is often seen in cases where prepaid cards have been used to facilitate criminal activities.

- Prepaid cards are **portable** and easily transported **cross-border**. The current definition of cash and bearer negotiable instruments in the Customs and Excise (Jersey) Law 1999 does not extend to prepaid cards and there is no requirement to report mailing or shipping such cards abroad. Furthermore, it can be difficult for law enforcement, customs, or border guards to determine and potentially seize the monetary value stored on a prepaid card. This is particularly relevant when prepaid cards have high load limits and are used to transport the proceeds of criminal activities;
- Ownership of the card may be transferred to an **unidentified bearer** (i.e., from the *customer* to another person);
- Prepaid cards may be purchased, and funds loaded, reloaded, redeemed, or withdrawn on a **non-face-to-face basis;**
- Prepaid cards may be **funded by cash** which could be the proceeds of criminal activity. Cards also provide **access to cash** by way of *ATMs*, "**cash back**" functionality or redemption;
- Prepaid cards may **be funded by unidentified third parties** and by other electronic products;
- The card may have a **high transaction limit** or **no transaction limit** at all. Prepaid cards that allow high values to be loaded, have high or no transaction value limits and high or no transaction frequency limits increase the risk of *money laundering,* the *financing of terrorism,* or the *financing of proliferation;*
- Individual *customers* or groups of *customers* may hold, have access to, or control **multiple cards**. Multiple cards can be transported or sent across borders in an attempt to circumvent the usual controls of cross-border cash movements;
- Prepaid cards may be used to make **frequent or high value cross-border transactions** by allowing *customers* to use funds loaded on their cards to be transferred onwards to other persons (person to person or business to business transfers);

- Most prepaid card programmes involve a number of agents which may be based in several different countries and territories. As a result of this segmentation there may be a **lack of consistent *CDD* measures** being applied across the issuer's business;
- Prepaid card operators typically **outsource business and compliance functions** to overseas locations, where the legislation **may not necessarily follow international standards**.

109. **Case study: Use of prepaid cards to launder the proceeds of crime**

- Prepaid currency cards have been used by individuals in Jersey to launder the proceeds of drug trafficking. For example, prosecutions in 2013 were connected with the laundering of criminal proceeds, amounting to £157,000, in Jersey through foreign currency exchange operators and through multiple loadings of criminal funds onto prepaid cards. In the case of the latter method, funds loaded locally were then withdrawn overseas, over a period of 34 months.
- Evidence demonstrated that individuals hired by the drug dealer were asked to "bank" the proceeds of illicit drugs sales by obtaining prepaid cards (two individuals held two cards each in their own names), loading cash onto these prepaid cards in Jersey, and subsequently withdrawing these funds in the UK and Spain.
- This case shows that criminals will exploit the different functionalities offered by prepaid cards. The ability to obtain multiple cards and load them with third party cash, the portability of such cards, and the ability to withdraw cash abroad have proved attractive to criminals.

14.2.5 Regulatory framework – prudential and conduct of business

Overview

110. There is currently no prudential or conduct of business regime in place in Jersey covering prepaid card issuers. However, in certain circumstances it is possible that prepaid card activity may fall within other regulatory regimes established, for example under the *BB(J) Law* (deposit-taking) or the *FS(J) Law* (where funds loaded on to a card are held by a card issuer in a trustee capacity).

14.2.6 Regulatory framework – *AML/CFT/CPF*

Overview

111. The activity of issuing prepaid cards is listed in paragraph 6 of Part 2 of Schedule 2 to the *Proceeds of Crime Law*: "Means of payment" issuing and administering means of payment (such as credit and debit cards, cheques, travellers' cheques, money orders and bankers' drafts, and electronic money)".

112. As a result, any person issuing electronic money (including prepaid cards) in or from within Jersey (directly or through an agent) or through a legal person established under Jersey law:

- becomes a *supervised person* for the purposes of the *Money Laundering Order* and is required to apply *CDD* measures, keep records, appoint an *MLCO* and *MLRO*, and to have *policies and procedures* in place to prevent and detect *money laundering,* the *financing of terrorism,* and the *financing of proliferation*;
- is required to register with the *JFSC* under the *Supervisory Bodies Law* or, where the person carries on a *regulated business* as defined in the *Supervisory Bodies Law*, to notify the *JFSC* that it is issuing prepaid cards; and
- is subject to supervision by the *JFSC* under the *Supervisory Bodies Law* for compliance with the *Money Laundering Order* and *AML/CFT/CPF Codes of Practice*.

113. The *Money Laundering Order* therefore **applies to prepaid card issuers with no physical presence in Jersey** that issue cards through Jersey-based agents.

114. The *Money Laundering Order* does not provide for the application of simplified *identification measures* to prepaid card *customers*. Prepaid card issuers are required to apply *CDD* measures to each *customer* and each third party on whose behalf the *customer* acts.

115. Where a *business relationship* is established with a *customer*, a prepaid card issuer is required to monitor *customer* transactions undertaken throughout the course of that *business relationship*.

116. By virtue of Article 2(3) of the *EU Regulation*, payment cards (among other methods of transfer) are exempt from the scope of the *Wire Transfers Regulations* where they are used exclusively for the purchase of goods or services and the number of the card accompanies all transfers. However, Article 2(3) of the *EU Regulation* also states that the use of a payment card to affect a person-to-person transfer of funds falls within the scope of the *EU Regulation*.

117. This means that where they satisfy the conditions set out in Article 2(3) of the *EU Regulation*, a person carrying on activities listed in paragraph 6 of Part 2 of Schedule 2 to the *Proceeds of Crime Law* is exempt from the obligation to include information on the payer in a wire transfer.

15 *AMLSP*S AND THEIR CUSTOMERS

15.1 Overview of section

1. This section applies only to *supervised persons who* are eligible to appoint *an AMLSP* in accordance with the Notice issued under Article 9A(4) of the *Money Laundering Order* (**Article 9A(4) Notice**).

2. An individual or organisation which is a *supervised person* may itself fulfil its own *AML/CFT/CPF obligations.* Alternatively, it may engage the services of an *AMLSP* and/or outsource within its group or to a third party (an outsourcing services provider) to assist it in meeting certain *AML/CFT/CPF obligations*.

3. The use of an *AMLSP* will not be subject *JFSC*'s Outsourcing Policy. The use of any other party, whether within the same group of the *supervised person* or not, is outsourcing and will be subject to the *JFSC*'s Outsourcing Policy. Section 18 of *this Handbook* will not apply to such outsourcing arrangements.

4. The provision of *MLRO/MLCO* roles to a *supervised person* may be undertaken by an *AMLSP*. It cannot however be outsourced within the *AMLSPs* wider group or to a third party.

5. Where a *supervised person* engages the services of an *AMLSP*, they shall be an *AMLSP Direct Customer*.

6. This section outlines the statutory provisions concerning the *AMLSP*. It also sets out the *AML/CFT/CPF Codes of Practice* and provides guidance on the obligations of an *AMLSP* and how an *AMLSP* might assist an *AMLSP Direct Customer* in fulfilling its *AML/CFT/CPF obligations*.

7. It is expected that the *AMLSP Direct Customer* will use the *AMLSP* to enable it to meet most of its *AML/CFT/CPF obligations*.

8. The *AMLSP Direct Customer* bears the ultimate responsibility for the activities undertaken in its name. This will include the requirement to determine that the *AMLSP* has in place satisfactory *systems and controls* (including *policies and procedures*), and that those *systems and controls* (including *policies and procedures*) are kept up to date to reflect changes in requirements.

9. For the purposes of fitness and propriety checks of key persons, as outlined in Section 10.6, individuals appointed by the AMLSP to the roles of MLCO and MLRO shall be referred to collectively as key persons.

15.2 *AMLSPs*

15.2.1 *AMLSP* systems and controls

AML/CFT/CPF Codes of Practice

[COP127] An *AMLSP* must include consideration of its *AMLSP services* within:

- its *BRA*;
- its formal strategy to counter *money laundering*, the *financing of terrorism*, or the financing of proliferation (*AML/CFT/CPF* strategy); and
- its systems and controls (including policies and procedures).

[COP128] An *AMLSP* must consider *AMLSP Indirect Customers* as if they were its own *customer*s when providing *AMLSP services*.

[COP129] Considering the conclusions of the *BRA* and *AML/CFT/CPF* strategy as they relate to the *AMLSP services,* the *AMLSP* must:

- organise and control its affairs in a way that effectively mitigates the risks that it has identified, including areas that are complex; and
- be able to demonstrate the existence of adequate and effective systems and controls (including policies and procedures) to counter *money laundering*, the *financing of terrorism*, or the financing of proliferation.

[COP130] An *AMLSP* must assess possible *money laundering, terrorist financing,* or *proliferation financing* risk associated with sub-outsourced functions, record its assessment, and monitor any risk on an ongoing basis.

Guidance notes

10. An *AMLSP* may demonstrate consideration of its *AMLSP services* within its *BRA*, *AML/CFT/CPF* strategy, and *systems and controls* (including *policies and procedures*) by clearly documenting the *AMLSP services* that it provides for its *AMLSP Direct Customers* and determining whether there are any differences arising from the provision of *AMLSP services* for its *AMLSP Direct Customers* by comparison to the *AML/CFT/CPF* activities that the *AMLSP* performs for its other *customers*.

11. For example, if there is clear documentation showing that the *AMLSP services* provided for *AMLSP Direct Customers* feature the same activities in respect of *AMLSP Indirect Customers* that the *AMLSP* performs for its other *customer*s then this may be taken to indicate that the *AMLSP* has considered its *AMLSP services* within its *BRA*, *AML/CFT/CPF* strategy and *systems and controls* (including *policies and procedures*).

12. Where the activities of an *AMLSP Direct Customer* are similar in nature to an *AMLSP's* other *customer*s extending the *AMLSP's BRA, AML/CFT/CPF* strategy and *systems and controls* (including *policies and procedures*) to include activities performed for *AMLSP Direct Customers* in respect of *AMLSP Indirect Customers* may be a natural extension.

13. Careful consideration of the following differences, and clear documentation of the measures taken to address these differences, may be taken to demonstrate that the *AMLSP* has properly considered *AMLSP Direct Customers*, and *AMLSP Indirect Customers*, in its *BRA, AML/CFT/CPF* strategy and *systems and controls* (including *policies and procedures*).

- Where the activities or operations of *AMLSP Direct Customers* are not similar in nature to an *AMLSP's* own activities or operations; or
- Where *AMLSP Indirect Customers* are not similar in nature to the other *customers* of an *AMLSP*.

14. An *AMLSP* may demonstrate consideration of *AMLSP Indirect Customers* as if they were its own *customers* by demonstrating the application of its *BRA, AML/CFT/CPF* strategy, and *systems and controls* (including *policies and procedures*) as amended for any differences in the nature of its *AMLSP Direct Customers*, and *AMLSP Indirect Customers* to its other *customers*.

15.2.2 *AMLSP* responsibilities

Statutory requirements (paraphrased wording)

15. *Article 9A(1) of the Money Laundering Order provides that a relevant person may appoint an AMLSP to appoint a MLCO and a MLRO and to comply with any other requirement of the relevant person under the Money Laundering Order.*

AML/CFT/CPF Codes of Practice

[COP131] The *AMLSP* must appoint an *employee* or *employees* to carry out the roles of *AMLSP Direct Customer MLCO* and *AMLSP Direct Customer MLRO* to each *AMLSP Direct Customer.* There can be no outsourcing of these roles by the *AMLSP*.

[COP132] The *AMLSP* must conduct relevant fitness and propriety checks including criminal records checks for existing and newly appointed key persons as expected in Section 10.6 on an ongoing basis on the AMLSPs appointed key persons.

[COP133] The *AMLSP* must make the appointment from a list of persons to whom the *JFSC* has provided its “no objection” in accordance with the Article 9A(4) Notice to such individuals being appointed as *AMLSP Direct Customer MLCOs* and *AMLSP Direct Customer MLROs,* and also notifying the *JFSC* of the removal of anyone from the list.

[COP134] The *AMLSP* need not supply the *JFSC* with updates on individual appointments into the roles for particular *AMLSP Direct Customers* but, must supply up to date information to the *JFSC* on request.

[COP135] The *AMLSP* must be able to demonstrate that it is providing services such that it has sufficient oversight and access to relevant information to appropriately manage the risks of providing the *AMLSP services* and to enable the *AMLSP Direct Customer MLCO* and the *AMLSP Direct Customer MLRO*, provided by the *AMLSP*, to fulfil their roles for the *AMLSP Direct Customer*.

[COP136] An *AMLSP* must provide sufficient information to satisfy an *AMLSP Direct Customer* that the *AMLSP* is fulfilling the *AML/CFT/CPF obligations* on an ongoing basis in accordance with the written agreement for services with the *AMLSP Direct Customer*.

[COP137] An *AMLSP* must demonstrate to its *AMLSP Direct Customer* how knowledge, suspicion, or reasonable grounds for knowledge or suspicion of *money laundering*, *terrorist financing*, or *proliferation financing* activity will be reported to the *AMLSP Direct Customer MLRO* (or their *Deputy*).

[COP138] An *AMLSP* must notify the *JFSC* and its *AMLSP Direct Customer,* immediately in writing of any material failures to comply with the requirements of the *Money Laundering Order* or the *AML/CFT/CPF Handbook* in respect of the *AMLSP services* it provides.

[COP139] An *AMLSP* must consider the effect that sub-outsourcing of activities that it performs as an *AMLSP* has on *money laundering*, *terrorist financing*, and *proliferation financing* risk, in particular where an *AMLSP Direct Customer MLCO* or *AMLSP Direct Customer MLRO* is provided with additional support from other parties, whether from within group or externally.

Guidance notes

16. The guidance in sections 2.3 and 2.4 of *this Handbook* will support *AMLSPs* in their approach to their general responsibilities.

17. Where it is deemed appropriate, considering the size and complexity of the *AMLSP Direct Customer*, the *JFSC* anticipates the same *Employee* could hold both *AMLSP Direct Customer MLCO* and *MLRO* roles.

18. Evidence to support compliance with the *AML/CFT/CPF Codes of Practice* at section 15.2.2 of *this Handbook* is likely to include:

- Documented consideration of *AMLSP services*, *AMLSP Direct Customers*, and *AMLSP Indirect Customers* within an *AMLSP's BRA*, *AML/CFT/CPF* strategy and *systems and controls* (including *policies and procedures*);
- A written agreement for services between an *AMLSP* and its *AMLSP Direct Customer* regarding the provision of *AMLSP services*; and
- Consideration of *AMLSP services* in the *AMLSP's* board minutes (or equivalent if the *AMLSP* is not a company).

15.2.3 *AMLSP Direct Customer MLCO*

Statutory requirements (paraphrased wording)

19. *Article 9A(2) of the Money Laundering Order provides that an AMLSP must fulfil the obligations of an AMLSP Direct Customer by appointing an Employee as MLCO.*

AML/CFT/CPF Codes of Practice

[COP140] An AMLSP must appoint an individual as AMLSP Direct Customer MLCO for an AMLSP Direct Customer that:

- is employed by the *AMLSP* or an enterprise in the same *financial group* as the *AMLSP*;
- is based in Jersey;
- has sufficient experience and skills.

[COP141] An *AMLSP* must ensure that the *AMLSP Direct Customer*'s MLCO:

- has appropriate independence, in particular from *customer*-facing, business development and *systems and controls* development roles;
- reports regularly and directly to the *MLCO* of the *AMLSP* (where they are not the same person) and has a sufficient level of authority within the *AMLSP* so that the *MLCO* of the *AMLSP* reacts to and acts upon reports made by the *AMLSP Direct Customer MLCO*;
- is able to raise issues directly with the *Governing body* of the *AMLSP Direct Customer*;
- has sufficient resources, including sufficient time and (if appropriate) a *Deputy AMLSP Direct Customer MLCO* and compliance support staff;
- is fully aware of their, the *AMLSP*'s, and the *AMLSP Direct Customer*'s *AML/CFT/CPF* obligations;
- formally acknowledges their appointment as *AMLSP Direct Customer MLCO* for each *AMLSP Direct Customer* to which they are appointed; and
- has sufficient access to information, oversight, and knowledge of the *AMLSP Direct Customer's* and the *AMLSP Indirect Customer's* activities on a continuing basis to fulfil the *MLCO* role.

- has undergone and will continue to confirm their fitness and propriety through criminal records checks conducted by the AMLSP on an ongoing basis.

[COP142] The *AMLSP Direct Customer MLCO*, the *AMLSP* and the *Governing body* of the *AMLSP Direct Customer* must ensure any proposed *AMLSP Direct Customer MLCO* has sufficient skills and experience to fulfil the role of *AMLSP Direct Customer MLCO* of the specific *AMLSP Direct Customer* to which they will be appointed.

[COP143] If the position of an *AMLSP Direct Customer*'s *MLCO* is expected to fall vacant, to comply with the statutory requirement to have an individual appointed to the office of *MLCO* at all times, an *AMLSP* must take action to appoint another appropriate member of senior management to the position on a temporary basis.

Guidance notes

20. Section 2.6 of *this Handbook* provides further information about the role of the *MLCO*.

21. An *AMLSP*'s *MLCO* may also be appointed as an *AMLSP Direct Customer MLCO*.

22. The appointment of an *AMLSP*'s *MLCO* as *AMLSP Direct Customer MLCO* is likely to be appropriate where the activities or operations of *AMLSP Direct Customer*s are similar in nature to an *AMLSP*'s other *customer*s, and where *AMLSP Indirect Customer*s are similar in nature to the other *customer*s of an *AMLSP*. In such circumstances, there is likely to be little difference between the *AMLSP*'s *BRA*, *AML/CFT/CPF* strategy and *systems and controls* (including *policies and procedures*) in respect of both the *AMLSP*'s own *AML/CFT/CPF* activities and the *AMLSP services* provided to its *AMLSP Direct Customer*s.

Statutory requirements (paraphrased wording)

23. *Article 9A(2) of the Money Laundering Order provides that an AMLSP must fulfil the obligations of an AMLSP Direct Customer by appointing an Employee as MLRO.*

AML/CFT/CPF Codes of Practice

[COP144] An AMLSP must appoint an individual as AMLSP Direct Customer MLRO for an AMLSP Direct Customer that:

- is employed by the *AMLSP* or an enterprise in the same *financial group* as the *AMLSP*;
- is based in Jersey;
- has sufficient experience and skills.

[COP145] An AMLSP must ensure that the AMLSP Direct Customer MLRO:

- has appropriate independence, in particular from *customer*-facing and business development roles;
- has a sufficient level of authority within the *AMLSP*;
- has sufficient resources, including sufficient time, and (if appropriate) is supported by *Deputy AMLSP Direct Customer MLROs*;
- is able to raise issues directly with the *Governing body* of the *AMLSP Direct Customer*;

- is fully aware of their, the *AMLSP*'s and the *AMLSP Direct Customer*'s *AML/CFT/CPF* obligations;
- formally acknowledges their appointment as *AMLSP Direct Customer MLRO* for each *AMLSP Direct Customer* to which they are appointed; and
- has sufficient access to information, oversight and knowledge of the *AMLSP Direct Customer's* activities and *AMLSP Indirect Customers* on a continuing basis to fulfil the *MLRO* role.
- has undergone criminal records checks and will continue to demonstrate their fitness and propriety through such checks conducted by the AMLSP on an ongoing basis.

[COP146] Where an *AMLSP* has appointed one or more Deputy *AMLSP Direct Customer MLRO*s the requirements set out above for the *AMLSP Direct Customer MLRO* must also be applied to any Deputy *AMLSP Direct Customer MLRO*s, save for the requirement to carry out criminal records checks.

[COP147] Where an *AMLSP* has appointed one or more Deputy *AMLSP Direct Customer MLRO*s, it must ensure that the *AMLSP Direct Customer MLRO*:

- keeps a record of all Deputy *AMLSP Direct Customer MLRO*s;
- provides support to, and routinely monitors the performance of, each Deputy *AMLSP Direct Customer MLRO*;
- considers and determines that SARs are being handled in an appropriate and consistent manner.

[COP148] The *AMLSP Direct Customer MLRO*, the *AMLSP* and the *Governing body* of the *AMLSP Direct Customer* must ensure any proposed *AMLSP Direct Customer MLRO* has sufficient skills and experience to fulfil the role of *AMLSP Direct Customer MLRO* of the specific *AMLSP Direct Customer* to which they will be appointed.

[COP149] If the position of *AMLSP Direct Customer MLRO* is expected to fall vacant, to comply with the *statutory requirement* to have an individual appointed to the office of *MLRO* at all times, an *AMLSP* must take action to appoint another appropriate member of senior management to the position on a temporary basis.

Guidance notes

24. Section 2.7 of *this Handbook* provides further information about the role of the *MLRO*.

25. An *AMLSP's MLRO* (or Deputies, as appropriate) may also be appointed as an *AMLSP Direct Customer MLRO.*

26. The appointment of an *AMLSP's MLRO* (or *Deputies,* as appropriate) as *AMLSP Direct Customer MLRO* is likely to be appropriate where the activities or operations of *AMLSP Direct Customers* are similar in nature to an *AMLSP's* other *customers*, and where *AMLSP Indirect Customers* are similar in nature to the other *customer*s of an *AMLSP*. In such circumstances, there is likely to be little difference between the *AMLSP's BRA*, *AML/CFT/CPF* strategy and *systems and controls* (including *policies and procedures)* in respect of both the *AMLSP's* own *AML/CFT/CPF* activities and the *AMLSP services* provided to its *AMLSP Direct Customers*.

27. To keep up with its obligations to have AMLSP appointed key persons that are fit and proper, an AMLSP may rely on the guidance provided to supervised persons in Section 10.6. which include that the AMLSP should be able to collect, the basic DBS checks (or foreign equivalent) on an ongoing basis using a risk-based approach.

15.3 *AMLSP Direct Customers*

15.3.1 *AMLSP* systems and controls

AML/CFT/CPF Codes of Practice

[COP150] Before engaging the services of an *AMLSP*, an *AMLSP Direct Customer* must be satisfied the *AMLSP:*

- Organises and controls its affairs in a way that effectively mitigates the risks that it has identified, including areas that are complex;
- Is able to demonstrate the existence of adequate and effective *systems and controls* (including *policies and procedures*) to counter *money laundering* and the *financing of terrorism* or *proliferation*; and
- Is able to perform the activities required to ensure the *AMLSP Direct Customer* fulfils its *AML/CFT/ CPF obligations.*

[COP151] On an ongoing basis, the *AMLSP Direct Customer* must ensure its *AML/CFT/CPF obligations* continue to be fulfilled by its *AMLSP* and must be able to demonstrate its oversight of the *AMLSP.*

Guidance notes

28. To satisfy itself an *AMLSP* and the *AMLSP Direct Customer MLRO and AMLSP Direct Customer MLCO* can perform the activities required, an *AMLSP Direct Customer* might ensure there is a written agreement in place between itself and its *AMLSP* that clearly sets out the scope of the *AMLSP services.* Such an agreement might include:

- Which *AML/CFT/CPF obligations* the *AMLSP* is responsible for fulfilling;
- How the *AMLSP services* are being fulfilled (service levels);
- Frequency and content of regular reporting b*y the AMLSP Direct Customer MLRO* and the *AMLSP Direct Customer MLCO* to the *AMLSP Direct Customer* board (or equivalent). Such reporting to be at a frequency in line with the risks assessed within the *AMLSP's BRA;*
- Actions to be taken on trigger events such as suspicions arising, or a change in the risk profile of an *AMLSP Indirect Customer*;
- Arrangements around suspicious activity reporting;
- The requirement for an *AMLSP Direct Customer* to consent to the sub-outsourcing of any of the *AMLSP services* undertaken by its *AMLSP*, if sub-outsourcing is to be permitted at all; and
- Clear acknowledgement of the *AMLSP Direct Customer's* ultimate responsibility for its own *AML/CFT/CPF obligations.*

29. The *JFSC* would expect to see, upon request, board minutes (or equivalent) of the *Governing body* of the *AMLSP Direct Customer* evidencing that it had carefully considered the appointments of its *AMLSP, AMLSP Direct Customer MLRO and AMLSP Direct Customer MLCO* prior to such appointments taking effect.

30. Demonstrating that the *AMLSP* is providing the services it has contracted to, and they are fulfilling the *AMLSP Direct Customer's AML/CFT/ CPF obligations* may be achieved through:

- the ongoing oversight of the *AMLSP Direct Customer's Governing body* of the *AMLSP services*. For example, if there is scheduled compliance reporting that this is complied with; and
- the *Governing body* of an *AMLSP Direct Customer* having participated in all relevant training provided by their *AMLSP* to its equivalent employees may support the *AMLSP Direct Customer* in demonstrating compliance with its *AML/CFT/CPF obligations*.

31. The *JFSC* would expect to see, upon request, board minutes (or equivalent) of the *Governing body* of the *AMLSP Direct Customer* evidencing the ongoing monitoring of services provided by the *AMLSP*.

15.3.2 *AMLSP Direct Customer* general responsibilities

Statutory Requirements

32. *Article 34 (2A) of the Supervisory Bodies Law provides that the registered person does not need to notify the JFSC of any changes in identity or convictions noted concerning an AMLSP appointed key person.*

AML/CFT/CPF Codes of Practice

[COP152] An *AMLSP Direct Customer* must be satisfied that knowledge, suspicion, or reasonable grounds for knowledge or suspicion of *money laundering* or *financing of terrorism* activity will be reported to the *AMLSP Direct Customer MLRO* (or *Deputy MLRO*).

[COP153] Where an AMLSP Direct Customer has AMLSP-appointed key persons, the *Direct Customer* is not required to notify the JFSC of their fitness and propriety unless:

i) specifically requested to do so by the JFSC,

ii) the notification forms part of an application for a no objection by the AMLSP, or

iii) another process beyond the scope of *Article 34* of the *Supervisory Bodies Law* requires it.

[COP154] Where an AMLSP is engaged to obtain criminal record certificates for key and principal persons, and not for the provision of key person roles, the registered person remains responsible for meeting their statutory obligations as outlined in section 10.6.

Guidance notes

33. An *AMLSP Direct Customer* could, when engaging with an *AMLSP* to assist in fulfilling its *AML/CFT/CPF obligations*, for example, use one of the methods set out in the below table, subject to appropriate risk-based modifications.

34. The *JFSC* recognises that it may not be appropriate in all cases for an *AMLSP Direct Customer* to adopt either of the two methods in totality or in part as set out below and a more bespoke approach may be required. For example, in complex high-risk scenarios.

Method 1	**Method 2**
AMLSP provides a form of *BRA, CRA*, and *policies and procedures* (in a similar form to its own) which can be adopted by the *AMLSP Direct Customer* as its own.	The *AMLSP* confirms and can demonstrate to the G*overning body* of the *AMLSP Direct Customer* that the *BRA*, *CRA*, and *policies and procedures* of the *AMLSP* address the risks associated with the *AMLSP Direct Customer's* business and *customers* (which includes *AMLSP Indirect Customers and* third parties for whom the *AMLSP Indirect Customers* act) as appropriate. For example, the *AMLSP CRA* of the *AMLSP Direct Customer* could be used as their *BRA*. In such instances the *Governing body* of the *AMLSP Direct Customer* would not need to adopt a separate *BRA, CRA* or *policies and procedures*.
AMLSP assists the *AMLSP Direct Customer* with the application of *CDD* measures at the outset of a relationship and on an ongoing basis in accordance with the *policies and procedures* of the *AMLSP Direct Customer* (which includes *AMLSP Indirect Customers and* third parties for whom the *AMLSP Indirect Customers* act).	*AMLSP* assists the *AMLSP Direct Customer* with the application of *CDD* measures at the outset of a relationship and on an ongoing basis in accordance with the *AMLSP's policies and procedures* (which will have been extended to make it clear that the *AMLSP* must carry out *CDD* in relation to each *customer* of the *AMLSP Direct Customer* and each third party for whom that *customer* acts).
AMLSP assists the *AMLSP Direct Customer* with the ongoing monitoring of the *AMLSP Direct Customer* (which includes *AMLSP Indirect Customers and* third parties for whom the *AMLSP Indirect Customers* act).	*AMLSP* assists the *AMLSP Direct Customer* with the ongoing monitoring of the *AMLSP Direct Customer* (which includes *AMLSP Indirect Customers and* third parties for whom the *AMLSP Indirect Customers* act).
The *AMLSP Direct Customer MLCO* carries out the *AML* compliance monitoring programme in accordance with the *AML* compliance monitoring programme of the *AMLSP Direct Customer* (in line with section 6 of *this Handbook*).	The *AMLSP* carries out its own *AML* compliance monitoring programme which will include ongoing monitoring in line with section 6 of *this Handbook*. The *AMLSP Direct Customer MLCO,* they should have the authority to request adjustment of the monitoring based on risk.
The *AMLSP Direct Customer MLCO* provides written periodic reporting at a frequency in line with the risks assessed of the *AMLSP Direct Customer* to the G*overning body* of the *AMLSP Direct Customer*.	The *AMLSP Direct Customer MLCO* provides written periodic reporting at a frequency in line with the risks assessed of the *AMLSP Direct Customer* to the G*overning body* of the *AMLSP Direct Customer*.

15.3.3 *AMLSP Direct Customer* – reserved activities

AML/CFT/CPF Codes of Practice

[COP155] The appointment of an *AMLSP* including the *AML/CFT/CPF* services to be provided by the *AMLSP* must be approved by the Governing body of the *AMLSP Direct Customer*.

[COP156] The Governing body of an *AMLSP Direct Customer* must approve any new business relationship (and continuation thereof) or one-off transaction where there is a connection to an enhanced risk state.

[COP157] An *AMLSP Direct Customer* that undergoes mergers, continuance, takeovers, or internal reorganisations, must ensure that records remain readily accessible and retrievable for the required periods in section 10 of *this Handbook*. This extends to the rationalising of computer systems and storage arrangements.

[COP158] Record-keeping arrangements must be agreed with the JFSC where an *AMLSP Direct Customer* terminates its activities or transfers *customer*s to another person.

Guidance notes

35. Reserved activities are activities that only the *AMLSP Direct Customer* can undertake.

36. Section 10 of *this Handbook* provides additional information regarding record-keeping arrangements.

15.3.4 *AMLSP Direct Customer* is a legal arrangement

AML/CFT/CPF Codes of Practice

[COP159] Where a Schedule 2 *activity* is conducted in relation to a legal arrangement, then the legal person, which is the *Governing body* of the legal arrangement, is responsible for the *AML/CFT/CPF obligations* of the legal arrangement. This applies whether the legal person is a corporate entity or a natural person.

[COP160] In some circumstances, the legal person, which is the *Governing body* of the legal arrangement, may have its own *AML/CFT/CPF obligations* in respect of the legal arrangement as well as *AML/CFT/CPF obligations* on behalf of the legal arrangement.

[COP161] *AMLSP services* provided to an *AMLSP Direct Customer* that is a legal person acting in relation to a legal arrangement may encompass both obligations. For example, where the legal person who is the *AMLSP Direct Customer* is acting in both the capacity of:

- A fund service provider/operator/functionary to the legal arrangement (the provision of *financial services* within the Schedule 2 definition of fund and security services activities and a trustee or general partner which will also be a Schedule 2 activity); and
- *Governing body* of the legal arrangement acting on behalf of the legal arrangement (participation in securities issues within the definition of fund and security services activities).

[COP162] This is a common arrangement in the funds sector, where for example there is a limited partnership that is a fund, and the general partner acts as both service provider to the fund as well as the *Governing body* of the fund.

[COP163] An AMLSP could provide the AMLSP Direct Customer MLCO and AMLSP Direct Customer MLRO to the AMLSP Direct Customer and this appointment could relate to both the AMLSP Direct Customer:

› In its own capacity; and

› Acting in relation to the legal arrangement.

[COP164] If the *AMLSP services* are to encompass a legal arrangement in relation to which the *AMLSP Direct Customer* is acting, the written agreement for *AMLSP services* is to be provided in relation to the legal arrangement.

[COP165] However, there may be circumstances where the *AMLSP Direct Customer*, or the *AMLSP*, will want to make differing arrangements in relation to those two roles because it may not be appropriate to fulfil both functions via the *AMLSP*. This is likely to depend on the level of complexity of the arrangement.

[COP166] Circumstances where the *AMLSP* is likely to fulfil the *AML/CFT/CPF obligations* for both the legal person and where the legal person is acting in relation to a legal arrangement may be where the *AMLSP Direct Customer* is acting as the *Governing body* for one legal arrangement. For example, where the *AMLSP Direct Customer* is a *SPV* trustee, or *SPV* general partner, without *employees* other than directors.

[COP167] Some examples of circumstances where a*n AMLSP* arrangement in respect of a legal person acting for itself and a legal arrangement may not be appropriate include:

› Where the trustee or the general partner are businesses with presence in the island which have their own *employees*;

› Where the trustees or the general partner provide services to multiple legal arrangements/funds; or

› Where the complexity, frequency or risks posed by the fund require a more subjective bespoke approach.

[COP168] Section 12 of *this Handbook* provides additional information regarding funds and fund operators, with section 13.2.4 of *this Handbook* regarding risk-assessments for *SPV* governing bodies providing guidance regarding potential approaches to the consolidation of risk assessments for legal arrangements.

16 VIRTUAL ASSET SERVICE PROVIDERS (VASPS)

16.1 Definition and overview of *VASPs* undertaking *supervised business*

1. Virtual Asset Service Providers (VASPs) are described in Part 4 of Schedule 2 of the Proceeds of Crime (Jersey) Law 1999 defining those services relating to virtual assets that fall under the scope of the *Money Laundering Order*. *Guidelines* provide the interpretation of VASPs and their activities.

2. Due to the fast transfer of value and cross-border transactions, VASPs must mitigate the risks of *money laundering*, *terrorist financing*, *proliferation financing*, and other illicit activities. This section includes specific risks and *money laundering* threats relating to VASPs and other VASP specific guidance.

16.2 VASP specific considerations

Overview

3. VASPs must comply with the same *AML/CTF/CPF* requirements as traditional financial institutions as outlined in Section 1 – 11 of *this Handbook*.

16.2.1 Risk assessment

4. This section is supplemental to, and should be read in conjunction with, Section 3.3.

5. Effective risk assessments and due diligence are essential, particularly when dealing with VASPs exposed to ML/TF/PF risks and foreign VASPs operating in jurisdictions that lack effective *AML/CFT/CPF* frameworks. VASPs should consider avoiding engaging with counterparties that cannot demonstrate effective *AML/CFT/CPF* measures.

6. The use of tools designed to increase anonymity (for example mixers, tumblers, privacy coins and decentralised platforms) increase risk exposure to illicit activities. Additionally, new illicit financing typologies continue to emerge that reduce transparency of transactions that are facilitated by Virtual Assets (VAs) as well as fiat currencies being converted to or from VAs. Therefore, VASPs should take caution to ensure that they investigate suspicious activities and patterns that may indicate emergent risks of ML/TF/PF or other illicit financing risks.

7. VASPs must stay vigilant against being used for layering virtual assets to obscure criminal activities, with risk assessment frameworks being regularly updated to reflect evolving risks.

16.2.1.1 Enhanced due diligence

8. This section is supplemental to, and should be read in conjunction with, Section 7.

9. On a risk basis VASPs are encouraged to collect additional information on high-risk *customer*s and transactions in order to identify, and avoid engaging in, prohibited activities, and to enable follow-up actions. Such additional information may include:

- the purpose of transaction or payment;
- details about the nature, end use or end user of the item;
- proof of funds ownership;

- parties to the transaction and the relationship between parties;
- sources of wealth and/or funds;
- the identity and the beneficial ownership of the counterparty; and
- export control information, such as copies of export-control or other licenses issued by the national export control authorities, and end-user certification.

10. Where a *VASP* is unable to verify the identity of an individual, it should consider not entering into a business relationship or executing a one-off transaction with that individual. If the business relationship already exists, the *VASP* may need to terminate the business relationship. In all circumstances, the *VASP* should consider filing a suspicious activity report in relation to the *customer* or individual.

16.2.2 Travel rule

11. *FATF* has called on jurisdictions to swiftly implement its “Travel Rule.” The Travel Rule requires transfers of virtual assets to be accompanied by accurate originator and beneficiary information. For more information refer to the *Travel Rule Guidance note* on the Jersey Financial Services Commission website.

16.2.3 Blockchain analysis

12. A *supervised person* may implement blockchain analysis to support in meeting their ongoing monitoring commitments as outlined within Section 6 of *this Handbook - Ongoing Monitoring*.

13. Blockchain analysis is a process of investigating, classifying, and monitoring blockchain addresses and transactions to understand the activities of various actors on the blockchain.

14. Blockchain analytics aim to provide transparency into blockchain transactions, including tracking them across different blockchains (i.e., across different crypto assets). They can also support the detection of suspicious activities, understanding transaction patterns, and modelling/visualising data. By analysing and visualising the full chain of transactions, these tools enable investigating entities to trace individual transactions back to identify the original source of funds and assess its legitimacy.

15. As blockchain and associated technologies are considered new and developing, the risks of using such technology to obtain evidence of identity should be considered, noting the particular characteristics of each application. This should be recorded in the BRA.

16. A *supervised person* may wish to implement a suite of monitoring methodologies incorporating new and traditional monitoring measures to ensure they mitigate risks associated with their *customer*s.

16.3 Money laundering typologies

17. Red flag indicators are crucial for detecting and preventing *financial crime* abuse in VASPs. These red flags are non-exhaustive indicative patterns or behaviours that may suggest potential involvement in illicit activities such as *money laundering*, terrorism financing or fraud. By recognising these signs, VASPs may implement effective measures to mitigate risks or cease activity with counterparties.

16.3.1 Red Flag Indicators Related to Transactions

16.3.1.1 Size and frequency of transactions

18. Structuring VA transactions in small amounts or amounts below record-keeping or reporting thresholds, similar to how cash transactions are structured

19. Conducting multiple high-value transactions in quick succession, such as within a 24-hour period, in a staggered and regular pattern, with no further transactions recorded for a long period afterward. This pattern is particularly common in ransomware-related cases or involves newly created or previously inactive accounts.

20. Transferring *VA*s immediately to multiple *VASP*s, especially those registered or operated in jurisdictions unrelated to where the *customer* lives or conducts business, or where *AML/CTF/CPF* regulations are weak or non-existent.

21. Depositing *VA*s at an exchange and then immediately withdrawing them without additional exchange activity, which incurs unnecessary transaction fees. This may also involve converting *VA*s to multiple types of *VA*s, again incurring additional fees without a logical business explanation (e.g., portfolio diversification), or withdrawing *VA*s from a *VASP* immediately to a private wallet. This effectively turns the exchange/*VASP* into a *money laundering mixer*.

22. Accepting funds suspected to be stolen or fraudulent, such as depositing funds from VA addresses identified as holding stolen funds or linked to holders of stolen funds.

16.3.2 Red Flag Indicators Related to Transaction Patterns

16.3.2.1 Transactions concerning new users

23. Making a large initial deposit to establish a new relationship with a *VASP*, where the amount deposited does not align with the *customer*'s profile.

24. Making a large initial deposit to open a new relationship with a *VASP*, funding the entire deposit on the first day, and then either trading/withdrawing the total amount or a significant portion of it on the same day or the next day.

16.3.2.2 Transactions concerning all users

25. Exhibiting abnormal transactional activity, such as high levels and volumes of VAs being cashed out at exchanges without a logistical business explanation.

26. Making frequent transfers to the same VA account within a specific period (e.g. a day, a week, a month) that involves multiple individuals; the same IP address used by one or more individuals; or a large amount of funds.

27. Receiving transactions from numerous unrelated wallets in relatively small amounts, accumulating funds, and then transferring them to another wallet or fully exchanging them for fiat currency. These transactions, conducted by several related accumulating accounts, may initially use VAs instead of fiat currency.

28. Conducting VA-to-fiat currency exchanges at a potential loss, such as when the value of VAs is fluctuating or despite abnormally high commission fees compared to industry standards, especially when there is no logical business explanation for the transactions.

29. Converting a large amount of fiat currency into VAs or converting a large amount of one type of VA into other types of VAs, without any logical business explanation.

16.3.3 Red Flag Indicators Related to Anonymity

30. Customers using multiple types of VAs, especially high anonymity VAs, despite higher transaction fees.

31. Transferring VAs to a centralised exchange and immediately trading them for higher anonymity VAs.

32. Abnormal levels and volumes of VAs cashed out at exchanges from P2P platform-associated wallets without a logical business explanation.

33. VAs transferred to or from wallets with patterns linked to mixing/tumbling services.

34. Transactions using mixing/tumbling services to obscure illicit fund flows.

35. Funds deposited or withdrawn from VA addresses or wallets with links to suspicious sources, including darknet marketplaces, mixing/tumbling services, questionable gambling sites, illegal activities and theft reports.

36. Using decentralised, un-hosted hardware, or paper wallets to transfer VAs across borders.

37. Users registering internet domain names through proxies or using domain name registrars that suppress or redact ownership details.

38. Users accessing VASP platforms using IP addresses associated with darknets or anonymous communication software (such as encrypted emails and VPNs)

39. A large number of seemingly unrelated VA wallets controlled from the same IP or MAC address, potentially using shell wallets registered to different users to conceal their relationship.

40. Using VAs with poorly documented designs or those linked to fraud or fraudulent schemes like Ponzi schemes.

41. Receiving funds from or sending funds to VASPs with weak or non-existent *CDD* processes.

16.3.4 Red Flag Indicators about Senders or Recipients

16.3.4.1 Irregularities observed during account creation

42. Creating multiple accounts under different names to bypass VASP trading or withdrawal limits.

43. Initiating transactions from suspicious or non-trusted IP addresses, including those from sanctioned jurisdictions.

44. Repeatedly attempting to open accounts within the same VASP from the same IP address.

45. Merchants or corporate users registering their internet domains in jurisdictions different from their establishment or in places with a weak domain registration process.

16.3.4.2 Irregularities observed during *CDD* process

46. Providing incomplete or insufficient CDD information or refusing to submit CDD documents or answer questions about source of funds.

47. The sender or recipient lacks knowledge or provide inaccurate information about the transaction, source of funds, or their relationship with the counterparty.

48. Submitting forged documents or altered photographs and identification documents during the onboarding process.

16.3.4.3 Profile of potential money mule or scam victims

49. A sender unfamiliar with VA technology or online custodial wallets.

50. An older *customer*, significantly above the average age of platform users, opens an account and conducts numerous transactions.

51. A financially vulnerable *customer*, often exploited by drug dealers to assist in trafficking activities.

52. A *customer* purchasing large amounts of VAs without substantial wealth or inconsistent with their financial history.

16.3.4.4 Other unusual behaviour

53. A *customer* frequently changes identification details, such as email addresses, IP addresses, or financial information, which may suggest an account takeover.

54. A *customer* attempts to access one or more VASPs from different IP addresses multiple times in a single day.

55. Language in VA message fields indicates transactions supporting illicit activities or the purchase of illegal goods, like drugs or stolen credit card information.

56. A *customer* repeatedly transacts with a specific group of individuals at significant profit or loss.

16.3.5 Red Flag Indicators in the Source of Funds or Wealth

57. Transaction with VA addresses or bank cards linked to fraud, extortion, ransomware, sanctioned addresses, darknet marketplaces, or other illicit website.

58. VA transactions involving online gambling services.

59. Using credit or debit cards linked to a VA wallet to withdraw large amounts of fiat currency or funding VA purchases with cash deposits into credit cards.

60. Deposits into an account or VA address significantly higher than usual with unknown sources, followed by conversion to fiat currency, indicating potential theft.

61. Lack of transparency or insufficient information on the origin and owners of funds, such as those with unavailable investor data, or incoming transactions from online payment systems through credit/pre-paid cards followed by instant withdrawal.

62. Customer funds sourced directly from third-party mixing services or wallet tumblers.

63. A *customer*'s wealth is primarily derived from investments in VAs or ICOs or other VASPs with weak AML/CFT controls.

16.3.6 Red Flag Indicators Related to Geographical Risks

64. Customer's funds are sent to or originate from an exchange not registered in the jurisdiction of either the *customer* or the exchange.

65. Customer uses a VA exchange or foreign-located MVTS in a high-risk jurisdiction or a jurisdiction with inadequate AML/CFT regulations.

66. Customer sends funds to VASPs in jurisdictions without adequate AML/CFT controls or VA regulation.

67. Customer establishes or relocates offices to jurisdictions without adequate AML/CFT controls or VA regulation, or where there is no clear rationale to establish/relocate office in that jurisdiction.

16.4 VASP terminology and glossary

16.4.1 Types of Virtual Assets

Type of Virtual Assets	Description
Utility tokens	VAs that grant digital access to specific digital platforms and to current or planned products or services. Typically, only accepted by the issuer or other users of a particular digital platform.
Payment/exchange tokens	Pseudo-anonymous: used as a means of exchange or potentially as a store of value. Transactions are linked to a specific sender.
	Anonymous (privacy coins): VAs with inbuilt anonymity features. Used as a means of exchange or potentially as a store of value. Transactions are not linked to a specific sender.
	Platform: used to access digital marketplaces and platforms. Also used as a means of exchange and potentially as a store of value.
	Asset-backed tokens (also known as stablecoins): VAs that purport to maintain a stable value by referencing more than one fiat currency, a commodity, or a basket of commodities and fiat currencies.
	Fiat-backed tokens (also known as stablecoins): VAs that purport to maintain a stable value by referencing a single fiat currency.
Closed-loop tokens	VAs used as a means of exchange within a closed system.

16.4.2 Types of Virtual Asset Service Providers

68. The World Bank has defined eight types of virtual asset service providers; however,, two are not defined as VASPs by the FATF. Nevertheless, the entity categories defined in the following table may interact with VAs or VA systems.

Type of Virtual Assets	Description
Wallet providers/custodians	Service providers enabling the storage of public and private keys.
Exchanges	Service providers facilitating virtual asset transfers and exchanges (VA - fiat / fiat - VA / VA - VA).
Payment processors and brokers, including orderbook exchanges	Service providers conducting payment processing/arranging transactions.
OTC desks	Service providers conducting payment processing/arranging transactions.
Asset management providers	Entities offering fund management/fund distribution.
Issuers	Entities issuing and selling VAs to the public.
Investment/trading platforms	Entities enabling investment in or the purchase of VAs via a managed investment scheme or a derivatives issuer providing VA options, or via a private equity vehicle that invests in VAs.

Miners/validators/pool operators*	Entities that validate and confirm transactions on a distributed ledger. Although not usually captured by the VASP definition, if they hold sufficient control/validation power, they could be considered VASPs.
Technology and ancillary service providers*	Entities offering mixing services, blockchain explorers, web administration, mining hosting services, information providers.

*Not covered by FATF recommendations

16.4.3 VASP risk exposure

69. The risks of *money laundering* associated with different types of virtual assets and virtual asset services may be considered as part of *Business Risk Assessment* of a *supervised person*. Example of considerations and higher risk factors is detailed below.

Feature of VA/VASP	Factors which may lead to higher risk of ML abuse
Anonymity	Anonymous Virtual Assets that prevent third parties from linking the VA to an identity.
Accessibility/liquidity	Virtual Assets that are highly liquid and are easily traded/exchanged and provide a more efficient mechanism to exchange or realise value.
Volume of trades	Higher volumes traded lead to higher liquidity levels and a wider range of VAs available to trade.
Amount of deposit/withdrawal	Deposits and withdrawals that involve the movement of larger amounts.
Method of trade	Trading is done via OTC desk (vs. order books). OTC desks may offer higher anonymity and may facilitate one-off transactions that do not require the establishment of a business relationship.
Customers	Private or anonymous individuals/entities rather than, for example, institutional investors and hedge funds.
Exchange used / asset pooling	› Unregulated exchanges used instead of regulated exchanges. › Decentralised exchanges that pool funds (limited traceability) and facilitate peer to peer trading without the governance of an intermediary.
Issuer	Weak controls or lacking AML/CFT processes by issuers allowing easy access to criminals.

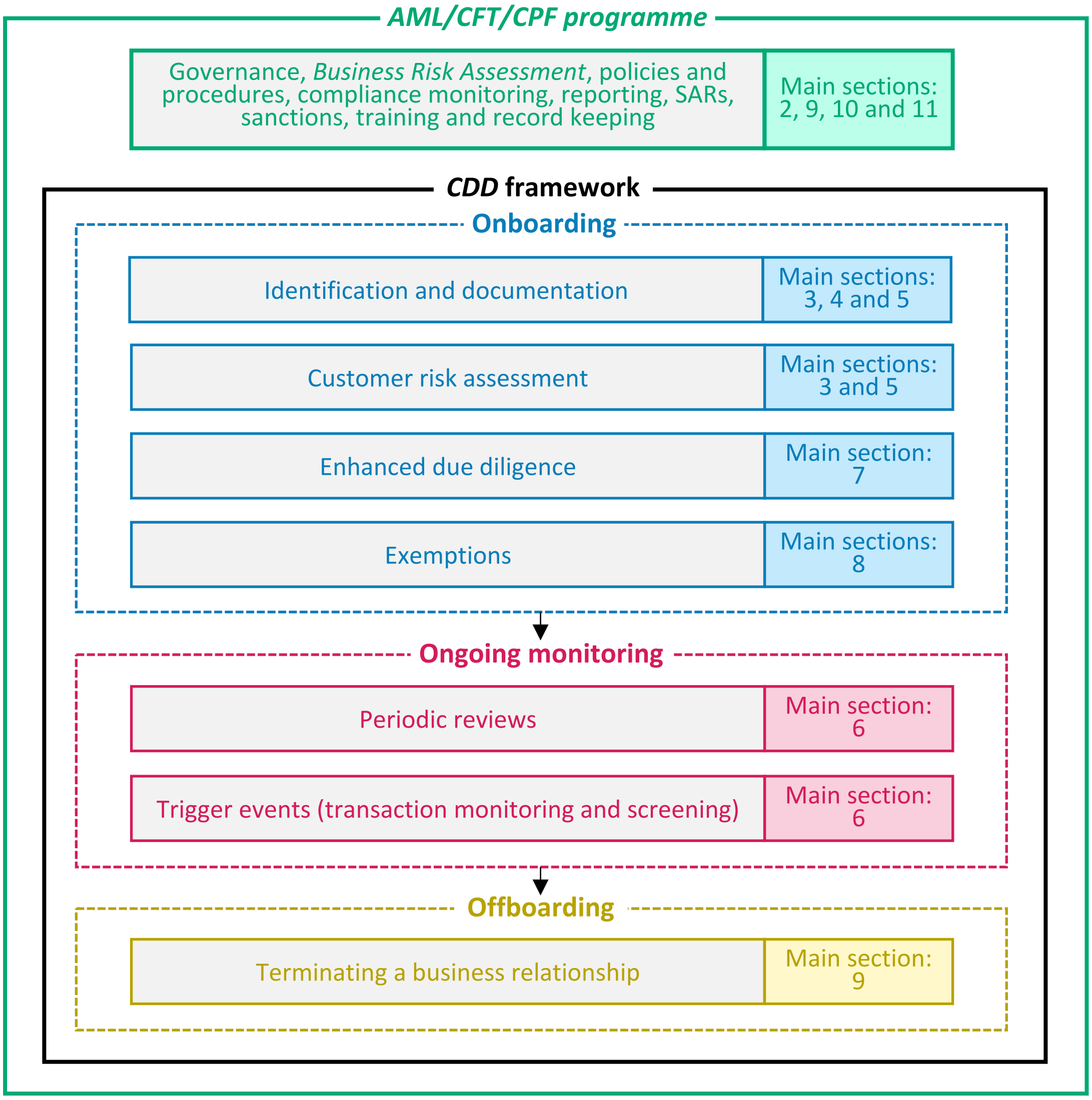
70. The above is an example of *money laundering* risks, but VA and VASP services should be assessed by *supervised persons* independently as part of their *Business Risk Assessment*. There is no specific profile in which criminal enterprise abuses Virtual Assets for ML purposes.

PART III: DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONALS (*DNFBPs*)

Industry	Section
Introduction to *DNFBP*s	17
Real estate agents	18
High value dealers	19
Lawyers	20
Accountants	21

17 OBLIGATIONS OF NOTE FOR ALL *DNFBPS*

1. Sections 1-11 are applicable to all entities/sectors classified as *supervised persons* and sections 17 – 21 apply to specific *DNFBP*s. High level mapping of the sectors to key processes in an *AML/CFT/CPF* programme are outlined below, which forms the content outlined in 'Part I: General Guidance':



2. **Important note**: Sections 17.1 and 17.2 are not intended to be a complete list of obligations for all *DNFBP*s, they are included to provide additional details and guidance over specific areas of note. This does not supersede the obligations and guidance outlined in Sections 1 - 11 of *this Handbook* but is intended to provide enhanced guidance over specific obligations.

17.1 Timing of *identification measures*

Overview

3. This section is supplementary to and should be read in conjunction with section 4.7 of *this Handbook*.

4. This refers to finding out identity, and obtaining evidence of identity, for a business relationship or one-off transaction. This sits in wider *CDD* procedures which include amongst other activities: risk assessing, enhanced due diligence and ongoing monitoring.

5. Section 4.7 of *this Handbook* sets out statutory requirements under the *Money Laundering Order* regarding when *identification measures* must be applied, in respect of a *business relationship* or *one-off transaction*.

6. Article 13 of the *Money Laundering Order* requires a *supervised person* to apply *identification measures*:

- before the establishment of a *business relationship* or before carrying out a *one-off transaction*; and
- in the course of a *business relationship*, where the *supervised person* has doubts about the adequacy of information previously obtained under *identification measures*.

7. As noted in section 4.7 of *this Handbook*, Article 13(4) of the *Money Laundering Order* allows, in certain circumstances, a *supervised person* a reasonable timeframe to undertake the necessary enquiries for obtaining evidence of identity after the initial establishment of a business relationship. No similar concession is available for finding out identity. Where a reasonable excuse for the continued delay in obtaining evidence of identity cannot be provided; to comply with Article 14(2) of the *Money Laundering Order*, a *supervised person* must terminate the relationship (see section 4.8 of *this Handbook*).

17.1.1 Ongoing Monitoring

8. This section is supplemental to and should be read in conjunction with Section 6.

9. Where *supervised persons* are involved in longer matters, periodic reviews should be undertaken on a risk sensitive basis, to ensure no significant factors have changed. For example, new parties to the matter, change of ownership or control (including control by other means), new sources of funds, new beneficiaries.

17.1.2 Duration of relationship with a *customer*

10. This section is supplemental and should be read in conjunction with sections 1.6 and 3.2 of *this Handbook.*

11. A relationship is considered to be established as soon as a *supervised person* undertakes to act on instructions as to the operation of that relationship, for example, by receiving and accepting signed terms of business from the *customer*.

12. In the case of *real estate agents, high value dealers, Accountants* and *Lawyers* this means a *business relationship* established before the *Money Laundering Order* came into force on 1 May 2008 and which continues. Refer to section 4.9.2 for further details on legacy *customer*s.

AML/CFT/CPF Codes of Practice

[COP169] A *supervised person* must not permit final agreements to be signed or pay away funds to an external party (or to another account in the name of the *customer*), other than to deposit the funds on behalf of the *customer*, until such time as evidence of identity has been obtained.

13. As noted above, where a relationship between a *supervised person* and a *customer* has no "element of duration" and is not a one-off transaction within the meaning of Article 4 of the *Money Laundering Order*, *identification measures* within the meaning of Article 13 of the *Money Laundering Order* are not required unless:

- The *supervised person* suspects *money laundering*, the *financing of terrorism* or the financing of proliferation; or
- The *supervised person* has doubts about the veracity or adequacy of any documents, data or information previously obtained under the *CDD* measures.

AML/CFT/CPF Codes of Practice

[COP170] In the circumstances set out in paragraph 13 above, the identity of the person undertaking the transaction must still be found out and recorded.

[COP171] A *supervised person* must record the basis that it has applied for determining the value of a transaction for the purposes of establishing whether it is a *one-off transaction* under Article 4 of the *Money Laundering Order*, and why that basis is appropriate.

[COP172] A *supervised person* must have in place measures to identify when linked transactions are being undertaken which would, in total, amount to €15,000 or more (for all *supervised persons* save for *MVTS*, *VASP*, or those operating a casino where different thresholds apply as set out in Article 4(1) of the *Money Laundering Order*), and therefore be a one-off transaction within the same meaning of Article 4 of the *Money Laundering Order*. *Supervised persons* must also consider when the frequency of regular *one-off transactions* by the same *customer* would constitute a *business relationship*.

[COP173] A *supervised person* must consider the nature of those transactions which are determined not to be a *one-off transaction* for which *identification measures* are not required. Where these transactions are considered to present a higher risk of *money laundering* or the *financing of terrorism* or *proliferation financing*, consideration must be given to applying full *CDD* measures.

[COP174] A *supervised person* must be able to demonstrate that their decision not to apply *identification measures* in respect of such transactions was reasonable considering its business risk profile.

17.2 Governance

14. The below are selected areas of focus and should be read in conjunction with sections 1 – 11 of *this handbook*.

AML/CFT/CPF Codes of Practice

[COP175] A *supervised person* must ensure that the *MLRO* maintains a record of all enquiries received from law enforcement authorities.

17.2.1 Business Risk Assessment (BRA)

Statutory requirements (paraphrased wording)

Activity	***Related statute (MLO)***
Business Risk Assessment	15. *Article 11(1)(f): A relevant person must maintain appropriate and consistent policies and procedure relating to risk assessment and management.*
	16. *Article 11(2)(a): Policies and procedures must take into account the level of risk identified in a national or sector-specific risk assessment in relation to money laundering carried out in respect of Jersey.*
	17. *Article 11(2)(b): Policies and procedures must take into account the type of customers, business relationships, products and transactions with which the relevant person's business is concerned.*

18. This section is supplemental and should be read in conjunction with sections 2.3 and 2.3.1 of *this Handbook.*

19. A *Business Risk Assessment* is a strategy document that assesses how exposed a *supervised person* may be to certain *financial crime* threats, and in turn, sets out how these threats and the associated risks of them occurring are mitigated and reduced.

20. The *BRA* relating to *customers* and services will depend on the *supervised person's* size, type of *customers* and the practice area it engages in or chooses not to. The *supervised person* should have a business risk appetite which will detail what the board have assessed and determined is beyond the *supervised person's* risk appetite, for example businesses where their profits are derived from selling weapons (see further guidance in Section 2.3.1)

21. *Supervised persons* should consider the different types of risk to which they are exposed. The risks should be considered within the context that a *supervised person* may be used to launder funds or assets through the *supervised person* or, alternatively, that the *customer* or its counterparties may launder criminal funds or assets.

22. As a minimum, a *Business Risk Assessment* should look to consider:

- The size and complexity of a *supervised person*, its day-to-day activities, who the *customer*s are, what kind of payments are received;
- a *supervised persons* organisational structure;
- a *supervised persons customer*s, and the countries and territories with which its *customer*s are connected;
- a *supervised persons* products and services, and how it delivers those products and services;
- the type of transactions a *supervised person* is subject to (for example, the use of cash and whether there is a limit to cash usage); and

- criteria for obtaining information from a client whose cash payment exceeds a certain threshold (either in a single transaction or several transactions which appear to be linked).

23. A BRA should document:

- how a *supervised person* plans to stay aware of the various kinds of criminal activities related to *money laundering*, *terrorist financing* and *proliferation financing and respective national risk assessments*;
- a record of the *supervised persons* staff training on understanding and identifying ML and TF risks, suspicious transactions and activity, and potential threats; and
- how the *supervised person* tests the knowledge and understanding it's staff have regarding the above points.

24. Specialisation within a sector that undertakes higher risk activity from a *money laundering, terrorist financing, and*/or *proliferation financing* perspective will affect the *BRA*. Examples of higher risk sectors and sensitive business areas for *money laundering*, the *financing of terrorism,* or the *financing of proliferation* purposes include:

- *financial services busines*ses (including *MVTS* activity);
- high cash turnover businesses: bars and clubs, taxi firms, launderettes, takeaway restaurants, market traders;
- gaming and gambling businesses;
- real estate and construction;
- computers and high technology, telecommunications, and mobile phone businesses;
- arms and armaments;
- activities related to cryptocurrencies and similar assets;
- antique/art dealerships (including auction houses); and
- dealers in high value or precious goods (e.g., jewels, gems, precious metals).

25. *Customers* who are *supervised persons* - such as *financial services businesses*, *MVTS* activity and *real estate agents* should have taken steps to mitigate their risks by implementing robust internal controls.

26. A non-exhaustive list of sector specific risks and threats are included in each sector specific section (13 – 21) which may be considered whilst building a BRA.

17.2.2 The *MLCO*

27. This section is supplemental to and should be read in conjunction with section 2.6 of *this Handbook*.

28. Section 2.6 of *this Handbook* sets out statutory requirements under the *Money Laundering Order* and *AML/CFT/CPF Codes of Practice* regarding the appointment of a *MLCO*.

17.2.3 The *MLRO*

29. This section is supplemental to and should be read in conjunction with section 2.7 of *this Handbook*.

30. Section 2.7 of *this Handbook* sets out statutory requirements under the *Money Laundering Order* and *AML/CFT/CPF Codes of Practice* regarding the appointment of a *MLRO* and, where relevant, *Deputy MLROs*.

17.2.4 Monitoring effectiveness of DNFBP's compliance

Statutory requirements (paraphrased wording)

Activity	***Related statute***
Compliance Monitoring Plan	31. *Article 11(2)(a): A relevant person must maintain adequate procedures for monitoring and testing the effectiveness of the following actions –* *(a) the policies and procedures maintained under paragraph (1);* *(b) the measures taken under paragraph (9); and* *(c) the training provided under paragraph (10).*

32. Because the BRA is a dynamic document it is necessary for the *supervised person* to devise a mechanism to monitor how effectively they implement preventative measures to mitigate the risks they are exposed to by their business. This is an ongoing process and is often described as a 'compliance monitoring programme'. Issues that should be considered as part of this process include:

- Procedures to be undertaken to monitor compliance, e.g. random file audits or file checklists to be completed before opening and closing a file whether periodic reviews of *CDD* are up to date;
- The frequency and content of reports that have been provided to senior management on compliance;
- How to rectify lack of compliance, when identified, and how remediation is monitored until completion and the metrics regarding this process; and
- How findings or lessons learned will be communicated to staff and fed back into the BRA of the business.

33. The resources allocated to appropriately implement the risk-based approach to *AML/CFT/CPF* compliance will vary. A small practice or sole practitioner is not expected to devote the same level of resources as a large practice. Having a smaller practice or being a sole practitioner with a smaller number of clients does not mean that this business is automatically lower risk. The risk of the business will depend on the type of work undertaken, the services provided, and the nature of the *customer*s. Smaller practices may be targeted by money launderers who may think they lack the resources to identify them.

34. Design of a robust CMP may include the following seven steps:

- identifying relevant legislative and regulatory requirements;
- identifying relevant controls;
- conducting a risk assessment;
- producing and approving a CMP;
- undertaking testing;

- reporting; and
- overseeing remedial action.

35. Under Article 11(12) of the *Money Laundering Order* the size and type of testing described above should be commensurate with the risk of *money laundering* that exists in respect of the *supervised persons* business and as such will vary between sectors, client types and services offered – which as outlined in 17.2.1 may be defined by the outputs from the BRA.

17.2.5 Non supervised business related activities

36. Whilst the *Money Laundering Order*, and consequently *this Handbook*, only brings within its scope the business activities where *DNFBP*s are carrying on a supervised business, the Anti-Money Laundering and Counter-Terrorism Legislation and the general offences and penalties cover all persons and all business activities within Jersey. Consequently, *DNFBP*s undertaking supervised business may wish to consider applying the systems and controls to counter *money laundering*, *the financing of terrorism,* or the *financing of proliferation* across the whole of their business activities.

18 REAL ESTATE AGENTS

18.1 Definition of *real estate agents* undertaking *supervised business*

Overview

1. Paragraph 19 of Part 3 of Schedule 2 to the *Proceeds of Crime Law* defines the relevant transactions and activity of *real estate agents* for the purposes of complying with the requirements of the *Money Laundering Order. Guidelines* provide the interpretation of "*real estate agents*" and their activities.

18.2 *Identification measures:* Finding out identity and obtaining evidence

18.2.1 Obligation to find out identity and obtain evidence

Overview

2. This sector-specific section is supplementary to and should be read in conjunction with section 4.2 of *this Handbook*.

3. A real estate agent or member of their staff may visit an individual at their home address. A record of this visit may corroborate the individual's residential address (for the purposes of a second document/source of verification). How and when this may be done should be included in the risk assessment and included in the real estate agents' policies and procedures.

AML/CFT/CPF Codes of Practice

[COP176] Following *FATF Recommendation* 22, a *supervised person* that provides real estate agency services as defined in paragraph 19 of Part 3 of Schedule 2 to the *Proceeds of Crime Law*, must comply with *CDD* obligations with respect to both purchasers **and** vendors of the property.

18.3 Exemptions from *CDD* measures – Jersey property transactions

Overview

4. This section is supplemental to and should be read in conjunction with section 8.3 of *this Handbook*.

5. This section relates to the exemption available under Article 18(6) of the *Money Laundering Order*, which provides that a *supervised person* that is a *Lawyer* or a *real estate agent*, which enters into a *business relationship* or carries out a *one-off transaction* for the purpose of enabling a *customer*, directly or indirectly, to enter into a registered contract within the meaning of the Control of Housing and Work (Jersey) Law 2012 (i.e. where it is to be passed before the Royal Court and registered in the Public Registry of Contracts), need not obtain **evidence of identity** of its *customer*.

6. Real estate agent specific exemptions:

Customer/Activity	Exemption	Article of MLO	Section of *this Handbook*	Conditions to be fulfilled before use?	Ongoing requirements?
Registered Property contracts passed before court	Customer	18(6)	8.3.7	Yes	Yes

AML/CFT/CPF Codes of Practice

[COP177] A *supervised person* that is a *real estate agent* must obtain and retain documentation establishing that its *customer* is entitled to benefit from the exemption set out in Article 18(6) of the *Money Laundering Order*.

18.4 Business risk assessment

18.4.1 Service area vulnerabilities and warning signs

Overview

7. Criminal conduct generates huge amounts of illicit capital, and these criminal proceeds need to be integrated into personal lifestyles and business operations. Law enforcement agencies advise that property purchases are one of the most frequently identified methods of *money laundering*. Property can be used either as a vehicle for *money laundering* or as a means of investing laundered funds.

8. Criminals will buy property both for their own use, e.g., as principal residences or second homes, business, or warehouse premises, and as investment vehicles to provide additional income.

9. The *BRA* relating to *customers* and services will depend on the *supervised person's* size, type of *customers* and the business area it engages in.

10. *Supervised persons* carrying on real estate agency business should consider the different types of *money laundering, financing of terrorism,* or the *financing of proliferation* risks to which they are exposed when providing services. This service area risk assessment must also be reflected when undertaking a *CRA*.

11. Further factors to consider when evaluating the risks posed by clients and service areas are set out in section 3.3.4 of *this Handbook*.

18.4.2 Criminal use of conveyancing services

Guidance notes

12. The *real estate agent* is but one of the professionals who will be involved in a property transaction. Every property transaction requires a legal practitioner to undertake the conveyancing, and this is one of the criminal's most frequently utilised functions. Conveyancing is a comparatively easy and efficient method of *laundering money* with relatively large amounts of criminal monies cleaned in one transaction. In a stable or rising property market, the *money launderer* will incur no financial loss except fees. Whilst many legal practitioners will be unwitting accomplices, some corrupt legal practitioners will provide deliberate assistance and *real estate agents* should be vigilant for any signs that this is occurring.

13. The purchase of real estate is commonly used as part of the last stage of *money laundering*. Such a purchase offers the criminal an investment which gives the appearance of financial stability. The purchase of a restaurant or hotel, for example, offers particular advantages, as it is often a cash-intensive business, which is the preferred currency of criminals. Cash remains the mainstay of much serious organised criminal activity. It has the obvious advantage that it leaves no audit trail and is the most reliable form of payment, as well as the most flexible. Retail businesses also provide a good front for criminal funds where legitimate earnings can be mixed with the proceeds of crime.

14. **Case Study 1: Drug Trafficking funds a hotel purchase**

- A financial intelligence unit received information that a previously convicted drug trafficker had made several investments in real estate and was planning to buy a hotel. An assessment of their financial situation did not reveal any legal source of income, and they were subsequently arrested and charged with an offence of *money laundering*. Further investigation substantiated the charge that part of the invested funds were proceeds of their own drug trafficking. They were charged with substantive drug trafficking, *money laundering* and other offences.
- The criminal's *Lawyer* received the equivalent of approximately US$70,000 cash from their *customer*, placed this money in their *customer's* bank account and later made payments and investments on the *customer's* instructions. They were charged with *money laundering* in relation to these transactions.
- The drug trafficker was convicted of drug trafficking, sentenced to seven-and-a-half year's imprisonment, and a confiscation order was made for US$450,000. The *Lawyer* was convicted and sentenced to 10 months imprisonment.

15. **Case Study 2: Tobacco smuggling funds a property empire**

- In 2005, a national assets recovery agency was granted an Interim Receiving Order by the courts for assets valued at over £1 million.
- The assets in question were held by Mr S and his wife. In its application to the courts, the Agency evidenced that Mr S purported to trade as an ice cream salesman with two vans. However, no street trading *Licence* had ever been granted making the vans recoverable property. The Agency also showed that on a number of occasions police had detected Mr S selling smuggled tobacco from his vans. His lifestyle and property acquisitions appeared to be far in excess of his lawful means.
- The assets included:
  - a principal residence in the capital city;
  - two apartments in the city centre;
  - an interest in a further eight building developments;
  - a planned apartment in a prestige city development.
- The Agency advised that they had intervened to prevent Mr S from extending his property portfolio shortly before the hearing.
- The total value of the property subject to the restraint order was estimated to be £1.4 million.

18.4.3 Recognising suspicious behaviour and unusual instructions

Overview

16. The following are examples of potentially suspicious events, both prior to and during the life of the property transaction.

18.4.3.1 **Absence of normal commercial rationale**

Guidance notes

17. Activity that does not appear to make good business sense may indicate that it is linked to criminal activity. For example, where the prospective purchaser is willing to pay significantly over the market value for a property, particularly where the purchase is being undertaken by a cash-rich company.

18. A property sale or purchase that is subject to any significant last-minute changes may indicate that there is an attempt to confuse the *CDD* information.

19. A *customer* that has no apparent reason for using a *supervised person* (for example the location of the property or type of business) where another business would be better placed to act, may indicate that the *customer* is trying to make it harder for *CDD* measures to be completed. Alternatively, the *customer* may hope that if the transaction is outside the normal size that a *supervised person* handles, or if it is particularly lucrative, the *supervised person* may turn a blind eye to any unusual or suspicious activity.

20. Where a *customer* has declined services that a *supervised person* would normally expect them to use, or shows little interest in the transaction, this may indicate that the property deal is a sham and merely being used to confuse the audit trail for criminal money (i.e., part of the "layering" stage of the *money laundering* process).

18.4.3.2 **Ownership issues**

Guidance notes

21. Properties owned by nominee companies or those with complex structures may be used as *money laundering* vehicles to disguise the true owner and/or confuse the audit trail. Last minute changes of instructions concerning the identity of the prospective purchaser in whose name the property is to be registered should give rise to additional due diligence.

22. Changes in the *beneficial ownership* of a company owning and managing a property where the new beneficial owners' *source of funds* for the company purchase is unclear or dubious may indicate that criminal funds have been injected into the company. This risk is heightened if known, reputable *Lawyers* have not been appointed by either or both sides to act for them.

23. Intermediaries may be used by criminals to protect their identity or hide their involvement. Real estate agents should be wary where ownership is said to be confidential and there is a reluctance to provide details of the *customer* for due diligence to be undertaken on them.

18.4.3.3 **Property values**

Guidance notes

24. A significant discrepancy between the sale price and what would be considered to be normal for such a property may indicate fraud or *money laundering*.

25. Properties sold below the market value to an associate may have the objective of obscuring the title to the property while the original owner still maintains the *beneficial ownership*.

26. There is a risk that transactions might be used for tax evasion, for example, the manipulation of property prices to just below the Stamp Duty threshold, perhaps by "rigging" the price of fixtures and fittings.

18.4.3.4 Valuations and surveys

Guidance notes

27. When *real estate agents* provide a valuation service prior to being instructed as selling agents, or when they are providing a service as surveyors, it is important that they are vigilant. If there is any indication that the property is being used for criminal conduct, a *SAR* must be submitted to the *MLRO*. A roomful of randomly stacked high value goods or a greenhouse inexplicably filled with cannabis cannot be ignored.

28. **Case Study 3: A lucrative farming enterprise**

› In 2006, a cannabis farm was discovered by local police. Officers found a large and sophisticated infrastructure for growing cannabis which could have produced close to £2.5 million pounds worth of cannabis over the previous four years. The owner, who was convicted of producing cannabis with intent to supply, was imprisoned for three years and had nearly £400,000 worth of assets confiscated.

18.4.3.5 Funding issues

Guidance notes

29. Whilst *Lawyers* will normally handle the funds provided for a property purchase, or the sale proceeds, *real estate agents* will often become aware of the funding arrangements. Suspicions should not be ignored merely because a *Lawyer* is also involved, and the sale or purchase funds are not passing through the *real estate agent's* client account.

30. For example, a *customer* who advises that the funds from the sale will be going overseas and paid to an unrelated third party may indicate that the funds are being laundered on behalf of that third party. Similarly, where the *source of funds* for a purchase is obscure or appears to be unusual, this may indicate *laundering* of criminal funds, particularly if the funds are offered in cash or are coming in from an overseas bank account that is unconnected to the purchaser.

31. A cash deposit paid to a *real estate agent* as part of a large property transaction, which is also to be settled in cash, may indicate tax evasion or that criminal proceeds are being used to fund the transaction. Cash is the principal currency of criminals and should always be subject to further enquiries.

32. Situations where a potential purchaser requests the real estate agent to hold the potential purchase funds in their client account must be treated with extreme caution. Because large amounts of cash cannot normally be banked without suspicions being raised, criminals will use other professionals as 'gatekeepers'. Placing cash into the banking system through client accounts of professional firms is a classic *money laundering* technique. Where a *customer* withdraws from a transaction after paying money into a client account, the *customer* receives a cheque or electronic transfer from the *Lawyer* or *real estate agent* which makes the funds appear to be legitimate.

33. *Real estate agents* should be mindful that as *Lawyers* tighten up on the circumstances in which they will hold *customer* money, other targets will be sought by criminals.

18.4.3.6 Mortgage fraud

Guidance notes

34. Where prospective property purchasers overstate or misrepresent their income to mislead mortgage lenders, this falls within the definition of mortgage fraud. Alternatively, the value of the property may be inflated with a view to obtaining a mortgage for the full inflated value. *Real estate agents* must avoid becoming complicit in such criminal arrangements. Mortgage fraud is itself a criminal offence, but if the *real estate agent* becomes involved, they are also entering into an arrangement to further a criminal act.

35. Unexplained changes in ownership may indicate a form of *money laundering* known as "flipping", which involves a property purchase, often using someone else's identity. The property is then quickly sold for a much higher price to the same buyer using another identity. The proceeds of crime are mixed with mortgage funds for the purchase. This process may be repeated several times.

36. Fraudulent borrowers will often seek to build a portfolio of properties by obtaining many mortgages with several lenders, using fictitious and/or real names. The portfolio is then used for various purposes such as:

- organised letting (particularly using assisted housing schemes);
- property development of a site or individual properties;
- 'rollover', where the criminal sells the properties to themselves (in various guises) at inflated prices.

37. Collusive mortgage fraud has become a significant problem in many countries with *real estate agents*, property valuers and legal professionals acting in concert to provide all concerned with maximum benefit.

38. **Case Study 4: Mortgage fraud investigation**

- A ring of over 40 professionals, including several fraudulent valuers, was broken because of an extensive mortgage fraud investigation. The fraudsters bought over 200 properties, falsely inflated their values, and sold them amongst themselves, fraudulently obtaining mortgages from most of the large lenders. No repayments were ever made on any of the mortgages which totalled over £30 million.

18.4.3.7 Buy to let

Guidance notes

39. Buy to let properties are particularly vulnerable to *money laundering* and especially so when linked to self-certification of income by the purchaser. Terrorist organisations may also purchase multi-tenanted property to provide safe haven accommodation for the operatives within their cells. The receipt of rent payments in cash also increases the vulnerabilities of letting agents.

40. To safeguard the position of letting agents who deal with buy to let properties or wish to receive payments of rent in cash, the Association of Residential Letting Agents has recommended that they voluntarily adopt the *AML/CFT/CPF systems and controls* (including *policies and procedures*) that are applicable to *real estate agents*.

41. **Case Study 5: *Money laundering* through buy to let**

› In 2004, following an investigation by law enforcement and tax authorities in the UK, several people were arrested for importing cannabis resin concealed in machines from overseas. One of the defendants offered to plead guilty if no confiscation order was brought against them. The investigation, which spanned several jurisdictions in Europe, had uncovered a property portfolio the defendant wanted to protect. The defendant had purchased several new apartments in various developments to launder the money and rent out the properties. A confiscation order was raised against the defendant amounting to nearly £3 million.

18.4.3.8 **Ghost lettings**

42. Ghost lettings raise *financial crime* risks and may take multiple forms:

- Where a property is being advertised for rent which is not available and this maybe without the knowledge of the homeowner or tenant;
- Multiple occupants living in a rental property unofficially – unauthorised sub-letting which may be to a criminal or for criminal purposes; or
- Where no-one physically occupies the premises when you would reasonably expect there to be an occupier, and rent is paid regularly.

18.4.4 Other *financial crime* red flags

43. *Financial crime* trends evolve, and real estate agents should consider what *money laundering terrorist financing* or proliferation risk they may face on a continuing basis. Other issues that may be relevant include:

- staff being offered bribes or becoming aware of bribes being made, for example, in relation to valuations or planning applications;
- acceptance of disproportionate corporate hospitality;
- owner of various properties using multiple agents without justification;
- virtual currencies being used to finance property transactions;
- searches on a party to a transaction or associate show, for example, adverse media attention, disqualification as a director, convictions for dishonesty or association with bribery in relation to contract procurement;
- cash exchanges directly between *customer*s e.g. for fixtures and fittings;
- poor explanation for the early redemption of a previous mortgage, especially where redemption incurs a penalty cost;
- the *customer* or counterparty does not take up services that are attractive or is willing to pay fees that seem unnecessary;
- the property value doesn't fit the *customer*'s profile;
- the client has not viewed the property or has only seen it on the internet;
- where multiple properties are purchased, resold or exchanged;
- a large cash deposit with the balance from an unusual source;
- multiple payments of smaller amounts possibly through different accounts and to avoid thresholds put in place by overseas authorities;

- unusual speed or requests to expedite transactions unnecessarily, possibly over or under value;
- a third party, apparently unconnected with the client bears the costs, settles invoices or otherwise pays the transaction costs;
- an unusually big cash or foreign currency transaction, and the buyer will not disclose the source of the funds;
- unusual involvement of third parties, cash gifts, or large payments from private funds, particularly where the buyer appears to have a low income;
- successive transactions, especially of the same property, with unexplained changes in value; or
- a previously sold property is re-marketed following renovation without an obvious source of funding.

19 *HIGH VALUE DEALERS*

19.1 Definition of *high value dealers* undertaking *supervised business*

Overview

1. Paragraph 20 of Part 3 of Schedule 2 to the *Proceeds of Crime Law* defines *high value dealers*, for the purposes of complying with the requirements of the *Money Laundering Order*.

2. *Guidelines* on the interpretation of "high value dealer" and activities and operations of *high value dealers.*

Guidance notes

3. Businesses registered as *high value dealers* need to apply the requirements of the *Money Laundering Order* to their transactions and activities on a risk-based approach. However, as part of demonstrating good practice, *high value dealers* may wish to consider applying *CDD* measures to any transactions and activity that will be paid in cash or *VA* with a value of £1,500 or more.

4. Any business that accepts cash or *VA* over the €15,000 threshold for relevant transactions (one transaction or a series of linked transactions) is required to register as a high value dealer. This means that any business that accepts payments in cash or *VA* of any amount needs to be aware of the threshold. Some businesses may decide that they will simply not accept payments over the threshold amount. Businesses that accept large amounts of cash or *VA* are vulnerable to money launderers as highlighted in the case studies above and below. Businesses that have decided not to register as *high value dealers* might support their decision by:

› A clearly documented policy known to all staff who accept payment that any significant cash or VA payments will be refused with payments only being accepted by other means (for example, by debit or credit card, or by bank transfer);

› A reasonable threshold, appropriate to the business, below the €15,000 maximum for which payments in cash or VA will be considered as significant, and refused;

› It is the *JFSC*'s expectation that this threshold for significant transactions would be approximately £1,500 or another amount that the business is able to clearly justify in its own circumstances;

› A method of being able to identify linked cash transactions to ensure they do not exceed the threshold.

5. Although the *high value dealer* population is varied, it mainly consists of retailers and wholesalers of goods who accept cash payments of €15,000 or more. Some common examples of goods subject to transactions by *high value dealers* include:

› Jewellery;

› art and antiques;

› precious metals;

› cars and yachts;

› agricultural goods.

Other examples of *high value dealers* include:

- retailers selling high-end electronics like tablets and smartphones;
- businesses selling alcohol and tobacco;
- wholesale/cash and carry businesses;
- businesses which supply tools and equipment to tradespersons, such as plumbers and electricians.

6. **Case study: Group *money laundering* – linked transactions**

- A group of criminals held £50,000 in cash obtained from drug trafficking operations. To launder their proceeds of crime, they targeted a high street jewellery business which held a high value dealer Licence. Over the course of a few days, each person in the group repeatedly visited the jewellery shop to purchase items. Whilst no one person spent more than €15,000 in any one transaction, together they laundered the full £50,000 into jewellery, which could then be enjoyed or re-sold for a profit.
- The staff who processed these transactions did not identify that the persons were operating together and therefore did not consider the total amount spent by the group. Nor did they realise that the transactions, whilst spread over multiple days, were linked to each other. As a result, they did not identify that the linked transactions carried out by this group exceeded €15,000.
- Had the business had more effective controls in place in line with *this Handbook*, they would have applied *CDD* measures to the group of money-launderers and may have formed a suspicion that *money laundering* was taking place.
- The business in this example appears to be involved in *money laundering* and may be found guilty of the offence of dealing with criminal property. The business also appears to have failed to have had adequate procedures to prevent and detect *money laundering* in line with the *Money Laundering Order*. As such, they may be found guilty of an offence of contravening or failing to comply with a requirement contained in any Order made under Article 37 of the Proceeds of Crime Law. In addition, the business may be found to have contravened *AML/CFT/CPF Codes of Practice* within *this Handbook* and therefore may be subject to proceedings by the JFSC.

7. Cash includes, for example, notes, coins, traveller's cheques, and bearer negotiable instruments. It does not include cheques or bankers drafts. Cash does not include payments by bank transfers, but it does include transactions in VA and cash payments directly into your bank account. As noted above the €15,000 threshold may be reached in respect of a single transaction or there may be several linked transactions that together total €15,000 or more.

8. Each business should assess, within its specific circumstances, which transactions it will consider to be linked for the purposes of preventing and detecting crime.

9. Transactions may be linked in the following scenarios (note this list is not exhaustive):

- they are executed by the same individual or group of individuals (including third parties connected with those persons);
- they involve the same asset;
- they occur across a specified time period, e.g., a high value item worth €15,000 or more is initially secured with a deposit, then the total value is paid in instalments over time;

- they appear designed to achieve an overarching objective (e.g., launder large sums of money);
- they do not have a commercial rationale (e.g., appear to be deliberately structured to avoid the €15,000 threshold);
- They are instalment payments for one item (e.g., cash instalments for a car) or against a single invoice.

10. It is important to note that whilst some transactions may appear to be linked from the outset, in other cases this may only become apparent at a later stage.

11. Each business should carefully assess and document the risks specific to its activities, traded goods, *customer* profiles and payment patterns.

12. Unusual sales or purchase activities may include:

- delivery methods or payment arrangements that are not consistent with normal practice;
- a new *customer* with little or no trading history and no trade references;
- a *customer* travelling to Jersey just to purchase goods, when the goods are readily available near their home location;
- a *customer* or representative making multiple smaller cash deposits into the business' bank account;
- unusual enquiries regarding the business' refund policy, e.g., *customer* asking if a refund can be made by cheque, wire transfer or paid to a third party.

13. **Case study: Less common goods sold by high value dealers**

- A couple involved in the distribution and sale of illegal substances attempted to launder £20,000 worth of proceeds from their illegal activities. They were handling bundles of Jersey £20 notes whilst trying to:
  - convert the cash into English notes.
  - deposit the cash into UK bank accounts.
  - purchase goods to be re-sold at a later date.
- The couple initially approached local banks. The banks followed their internal policies on handling cash and refused to accept a cash deposit due to the amount and unexplained/undocumented source. Similarly, the couple approached a local car dealership. The dealership was not registered as a high value dealer as its policy did not allow acceptance of significant cash payments. They refused to sell vehicles for cash. The couple then decided to approach a smaller retailer stocking a wide range of electronics. They subsequently purchased expensive laptops, computers, and smartphones.
- Despite the bill totalling over £20,000, the staff processing the transaction did not become suspicious and did not query the origin of the cash. It was later identified that the retailer did not have policies on accepting significant cash payments. Therefore, their staff were unaware of the cash value threshold set out in the *Proceeds of Crime Law*.
- The business was willing to accept transactions that fall within the *high value dealer* definition in the *Proceeds of Crime Law*. As such the electronics retailer should have been registered as a *high value dealer*. If they had been registered, they should have had appropriate *systems and controls* in place to identify the suspicious nature of the transaction. Had they been registered and had the relevant controls in place, the apparent *money laundering* above should have been identified. For example, the business would have applied *CDD* measures to the couple and may have formed a suspicion that *money laundering* was taking place.

› The business in this example appears to be involved in *money laundering* and may be found guilty of the offence of dealing with criminal property. The business also appears to be an unregistered high value dealer and may be found guilty of the offence of carrying on unauthorised *supervised business*. In addition, while they were not registered as a *high value dealer*, it appears that the business should have been registered with the *JFSC* so may be found to have contravened *AML/CFT/CPF Codes of Practice* within *this Handbook* and therefore may be subject to proceedings by the *JFSC*.

19.2 Business risk assessment

19.2.1 Service area vulnerabilities and warning signs

Overview

14. The *Business Risk Assessment* relating to *customers* and services will depend on the *supervised person's* size, type of *customers* and the business area it engages in.

15. *Supervised persons* carrying on the business of a *high value dealer* should consider the different types of *money laundering, financing of terrorism,* and *financing of proliferation* risks to which they are exposed when providing services. This service area risk assessment must also be reflected when undertaking a *CRA*.

16. Further factors to consider when evaluating the risks posed by clients and service areas are set out in section 3.3.4 of *this Handbook*.

19.2.2 Recognising suspicious behaviour and unusual transactions

Overview

17. Cash remains the mainstay of much serious organised criminal activity. It has the obvious advantage that it leaves no audit trail and is the most reliable form of payment, as well as the most flexible.

18. As illustrated in the following case study, the €500 note has become the bank note of choice for criminals, replacing the US $100 note. Consequently, *high value dealers* should always exercise additional vigilance when accepting a large number of €500 notes from any one *customer*.

19. **Case Study 6: Disappearing €500 notes**

› In 2005, the central bank of a European country advised that €500 notes were increasingly being drawn from high street banks and then disappearing. By 2006, 100 million more notes were issued to high street banks than were handed in by them. This was of significant concern because it meant the country was using over 25% of all €500 notes that were issued within the Eurozone;

› in response to the central bank's concern, an investigation was launched by the national government into the missing notes. The result was that the national treasury identified nearly 14,000 suspicious transactions totalling €6 billion that had taken place between 2003 and 2006 using €500 notes;

› for example, the deputy mayor of a seaside town was found to have nearly €400,000 in €500 notes in their safe when they were arrested by police in 2006 during the investigation of organised crime groups operating in the region.

20. Those in receipt of large sums of cash have the problem of how to dispose of it. The objective of the first stage of *money laundering* – placement – is to move the criminal cash into the financial system. It is extremely difficult to place large amounts of cash into the banking system without raising suspicions. Serious organised criminals frequently launder cash through legitimate and quasi legitimate businesses, typically those with a high cash turnover. The businesses are often owned or part–owned by the criminals or by close associates, although legitimate businesses may also be targeted to provide the means for *laundering* criminal proceeds. Retail businesses that genuinely accumulate and bank large amounts of cash are natural targets for *laundering* the cash though genuine purchases.

21. Businesses which find themselves in financial difficulties may also be targeted by criminals. Cash may be placed into the financial system by persuading the owners or managers of the business to deposit criminal money along with their normal takings. The business then transfers the criminal money to the *money launderer's* account, taking a cut along the way.

22. **Case Study 7: Disposal and exchange of cash**

› A number of banks in a European capital city were visited by the local drug squad;

› accounts had been opened for companies running cash-based businesses that received cash from *customers* and paid suppliers in cash;

› the businesses arranged to deliver cash to the banks in small denomination notes, which would then be exchanged for the larger €500 notes. The €500 notes were then either paid into other bank accounts or smuggled out of the country. No *SARs* had been made by any of the banks concerned.

19.2.2.1 Recognising stolen cash

Guidance notes

23. Stolen cash is frequently laundered through retail outlets. Sterling, and many euro banknotes, become stained with dye when cash boxes are stolen and opened during bank or cash-in-transit robberies. Criminals frequently attempt to clean the notes, but this damages the foil and other security features.

19.2.2.2 High value cash transactions

Guidance notes

24. *Money launderers* normally want to move funds quickly to avoid detection. This is more easily done in large one-off transactions. The purchase of high value goods, with good portability, paid for in cash, represents an attractive target for *money launderers*. Luxury goods paid for with cash that can easily be sold on (even at a loss) for "clean money" are especially attractive.

25. Equally an asset may be purchased to support a certain lifestyle (e.g., a high-performance car or a yacht). Alternatively, an asset may be purchased as a form of long-term investment (e.g., jewellery, an antiquity, a work of art etc.).

26. **Case Study 8: A high value lifestyle**

› In 2007, nearly £3 million was seized from two criminal families who made a fortune from car crime and tax evasion;

› The two families lived a life of luxury, shopping at Harrods and wearing designer clothes and jewellery and driving top of the range cars. However, it was all paid for through crime;

- The families made their money by dishonest car dealing – turning back the mileages of cars and then selling them on – and by selling stolen caravans. The scam involved forged documents, altered MOT certificates and fake service histories;
- The gang of eleven, none of whom had legitimate jobs, then made the money disappear by splashing out on luxury cars, designer jewellery, clothes, perfumes, chinaware and other antiques;
- When the homes of the gang were raided by 350 officers from four UK police forces, almost £1 million in cash, mostly in £50 notes, was found to be buried in the grounds or hidden around the various houses;
- Members of the gang pleaded guilty to *money laundering*, criminal conspiracy, obtaining money by deception and possessing criminal property.

19.2.2.3 Gold, precious metals, precious stones and jewellery

Guidance notes

27. Criminal funds can be used to purchase gold, which is then exported to other jurisdictions and sold, thus legitimising the funds as the proceeds of sale. The use of gold is attractive for many reasons – it is the only raw material comparable to money. It is a universally accepted medium of exchange which is traded on world markets and the *money launderer* can remain anonymous.

28. **Case Study 9: Gold moulded into tools**

- A New York gold refinery owner was found guilty of *laundering money* for Colombian drug traffickers by selling them gold moulded into tools, screws and other bulk items that could be shipped to Colombia undetected.

29. The jewellery trade can also become involved in *money laundering*. Precious stones and jewellery are easily transportable and highly concentrated forms of wealth.

30. **Case Study 10: *Money laundering* through gold and diamonds**

- A three-year investigation into drug *money laundering* in Manhattan's diamond district was undertaken. Dealers had agreed to trade 220 pounds of gold and diamonds for more than US$1 million in cash. The probe resulted in over 20 arrests, including 11 jewellers and the seizure of more than US$1.5 million in cash, US$1.3 million in gold and 118 kilograms of cocaine;
- One jeweller was charged with agreeing to exchange diamonds and gold for US$600,000 in cash.

31. **Case Study 11: Cross-border operation**

- Mr A was convicted in December 2020 of *money laundering* in connection with the importation and supply of drugs in in their jurisdiction. The wider investigation resulted in the seizure of drugs with a street value of around £900,000;
- Mr A owned and ran a jewellery business which allowed him to facilitate the movement of criminal property from their jurisdiction to the UK through the purchase and sale of bullion. This enabled cash to be removed from the country under the cover of legitimate transactions, and without the cash being physically carried out of the jurisdiction.
- The process was carried out in four steps:
  - A sum of cash, *from the sale of drugs*, would be handed to Mr A at his jewellery shop;
  - Mr A would deposit that cash into his personal and business bank accounts;

- Mr A would use the cash to purchase gold bullion from a dealer based in Hatton Garden in London;
- The gold would be collected from the London dealer and sold for cash.

› The cash would then be available to UK-based members of the criminal enterprise to be used to purchase drugs, or otherwise to cover the operating costs of the enterprise.

19.2.2.4 The motor trade

Guidance notes

32. Vehicles may be either the source of the laundered money or the means by which other illegal income is laundered. *Money launderers* often make contacts within trades where the use of cash is accepted, such as dealers in expensive cars.

33. **Case Study 12: Using cars to facilitate *money laundering***

› The financial intelligence unit of Country R received a *SAR* on large purchases of Country F currency totalling US$263,000 and carried out by a citizen of Country R;

› The funds in Country F currency were used for the purchase of new motor vehicles in Country F. However, the transactions detected appeared to include only part of the funds moved by the individual and their associates;

› Indeed, the organisation to which the individual belonged regularly acquired new motor vehicles in Country R for payments in cash from a large dealership – which was either in collusion with the organisation or turning a blind eye to the activity;

› The purchased vehicles (worth around US$30,900 each in the verified cases) were delivered and then driven to a neighbouring country where they were received by a close relative of the main individual in the scheme and known by authorities to be involved in narcotics trafficking. The vehicles were then exchanged for large quantities of drugs which were to be resold in Country R. Investigations revealed that the total amount of money involved in the scheme was more than US$355,000.

34. **Case Study 13: Car Importer committing tax evasion**

› Mr B bought and sold Porsche, BMW, Mercedes and other high value vehicles. He ordered the cars from mainland Europe and created a network of false identities and addresses to avoid paying import tax on the vehicles. Import documents gave false details and he built up a portfolio of false names and addresses from vehicle registration centres around the country. Police investigators traced the cars back to the importers. They found that numerous individuals had been paid £10 each to receive the vehicle registration documents through the post. Many of the cars were then sold for cash and were ultimately untraceable;

› As a result of the investigations, UK Police secured £1 million in assets following the conviction of Mr B who was jailed for two and a half years for *money laundering* and conspiracy to defraud the Revenue Authorities.

35. Outstanding finance is a big risk faced by dealers who buy second hand cars. HPI Limited have previously advised that 24 out of every 100 cars offered for sale that are checked by them are still subject to a finance agreement. If the loan remains unpaid when the vehicle is purchased, the second-hand dealer and any subsequent buyer will not acquire good title to it.

19.2.2.5 Behaviours indicative of suspicious transactions

Guidance notes

36. The following is a non-exhaustive list of examples of potentially suspicious transactions:

- reluctance to make personal contact;
- reluctance to provide the required identification information or evidence of identity;
- the size of purchase is out of line with the appearance/age of the *customer*;
- *customers* who initially indicate that they will be paying for goods over €15,000 by credit card/cheque and then at the last-minute present cash as the means of payment;
- there appear to be no genuine reasons for paying large sums of money in cash;
- cash is unusual for that type of *customer*;
- *customers* purchasing goods which are available nearer home at a similar price;
- purchases by businesses where the level of cash activity is higher than the underlying business would justify; and/or
- the *customer* is paying in small denomination used notes.

19.2.2.6 Goods that are returned for refund

Guidance notes

37. Returning high value goods paid for in cash and obtaining a refund by way of a cheque or electronic payment enables the *laundering* of the "dirty money" by exchanging it for a legitimate retailer's payment. As an example, suspicions may be raised in the following circumstances:

- the *customer* enquires about the *supervised person's* refund policy prior to purchasing;
- the *customer* seeks a refund for spurious reasons; and/or
- the *customer* seeks the repayment in the form of a cheque or electronic payment when the purchase or a deposit was made in cash.

38. **Case Study 14: The cash deposit scam**

- A professional criminal *money launderer* developed a simple technique of going into several high-priced West End jewellers and asking to inspect very expensive pieces of jewellery, saying that he was looking for a present for his wife. Dressed expensively and presenting himself well, he would choose various pieces and then ask to see the manager. Explaining that he wanted to give his wife the opportunity to choose for herself, he asked if the shop would be prepared to take the items off display and hold them for his wife's inspection. He explained that he would be prepared to deposit significant sums of cash to be held by the shop as a deposit for the items chosen, and that once his wife had chosen the item she wished, he would pay the balance. He also explained that any sums uncollected could be returned to him in the form of a cheque made payable to one of his corporate entities;
- On five separate occasions he placed significant sums of cash, a total more than £100,000, as 'deposits' for items of valuable jewellery. On each occasion, his 'wife' then went into the shop on the following day and inspected the relevant items. Finding nothing to her taste, she then asked the store to make a cheque payable to her husband's business as previously instructed;

› Both husband and wife were later arrested after one store learned about the unusual couple with so much money to spend but with such particular tastes. They shared the information among their trade members and discovered that the tactic had been used on several previous occasions. They then alerted the police.

39. **Case Study 15: Cash into wine**

› A similar technique was discovered by a leading wine trade company who discovered that a number of apparently wealthy businessmen were asking to buy significant volumes of high-value wine, and keeping it held in 'bond' by the firm. The businessmen paid for their purchases in cash but did not ask for the wine to be released from the bonded warehouse. This was not considered unusual as many wine buyers purchase investment wines in this way. Later, upon request, the businessmen asked for their wines to be re-sold back to the company, sometimes at enhanced rates, depending upon the prevailing sale-room price.

19.2.2.7 **Buying second-hand goods**

Guidance notes

40. *High value dealers* who buy high value second-hand items for trading on should be vigilant to avoid handling stolen property. A *money launderer* who has exchanged criminal cash for a high value asset and then trades it in has a cheque that can be paid into their bank account. They have therefore effectively 'placed' and 'integrated' the laundered money. Jewellers, art, and antique dealers should use their networking to exchange information when stolen goods are being offered around for sale. Transactions using virtual assets *High value dealers* who transact in *virtual assets* will need to consider if they need to register. For example, some dealers are advertising that jewellery or art may be purchased using cryptocurrency. The thresholds for cryptocurrency/virtual assets are the same for cash singular transaction or linked transactions of €15,000.

20 *LAWYERS*

20.1 Definition of *Lawyers* undertaking *Supervised business*

20.1.1 Activities to which the *Money Laundering Order* applies

Overview

1. Paragraph 21 of Part 3 of Schedule 2 to the Proceeds of Crime Law defines the relevant operations and activities of lawyers, notaries, and other independent legal professionals (Lawyers) for the purposes of complying with the requirements of the *Money Laundering Order*. Guidelines provide the interpretation and activities and operations of Lawyers that are in scope.

2. Whilst the *Money Laundering Order*, the *Guidelines* and consequently *this Handbook*, only brings within its scope the business activities of law firms where they are carrying on a *supervised business*, the *Anti-Money Laundering and Counter-Terrorism Legislation* and the general offences and penalties cover all persons and all business activities within Jersey. Consequently, law firms undertaking a significant proportion of *supervised business* may wish to consider applying the *systems and controls* to counter *money laundering,* the *financing of terrorism,* or the *financing of proliferation* across the whole of their business activities.

20.2 *Identification measures*

20.2.1 Urgent undertakings

3. Section 4.7 of *this Handbook* sets out statutory requirements under the *Money Laundering Order* regarding when *identification measures* must be applied, in respect of a *business relationship* or *one-off transaction*.

4. Where the provision of *supervised business* by a *Lawyer* is urgent, this undertaking may be provided prior to obtaining evidence of identity if there is little risk of *money laundering, the financing of terrorism, or proliferation financing* occurring, and evidence of identity is obtained as soon as reasonably practicable. Nevertheless, identity is still required to be **found out**.

5. For clarity the above includes:

› There is little risk of *money laundering*, and the relationship/transaction should not be deemed high risk;

› Timeline for obtaining evidence of identity must be reasonably practicable (i.e. the timeline for obtaining evidence must be justifiable);

› There is a genuine reason for urgency, and the above is used on an exceptional basis for urgent business only and not for business as usual.

20.2.2 Ascertaining legal position

Overview

6. Section 4.8 above sets out the statutory requirements under the *Money Laundering Order* to terminate a *business relationship* or not carry out a *one-off transaction* where a *supervised person* is unable to apply *identification measures* in respect of that relationship or one-off transaction.

7. A concession from terminating a *business relationship* is permitted for *Accountant*s, *Lawyers* and other professional advisers who are in the course of ascertaining the legal position for their *customer* or performing the task of defending or representing their *customer* in legal proceedings (including advice on instigating or avoiding proceedings).

8. To qualify for the concession the *Accountant*, *Lawyer* or other professional adviser must be a member of a relevant professional body that undertakes competency testing for its members and imposes and maintains professional and ethical standards.

Statutory requirements (paraphrased wording)

9. *Article 14(9) of the Money Laundering Order provides that the prohibition from continuing a business relationship does not apply where the relevant person is a lawyer or other business falling within paragraphs 21 or 22 of Part 3 of* Schedule 2 *to the Proceeds of Crime Law and is in the course of ascertaining the legal position for that person's client or performing the task of defending or representing the client in, or concerning legal proceedings, including advice on instituting or avoiding proceedings.*

Guidance notes

10. *CDD* information will still need to be collected within a reasonable timescale to comply with Article 13 of the *Money Laundering Order*.

11. *Accountants*, *Lawyers*, and other relevant professional advisers are encouraged to consider their position very carefully before applying the above concession to ensure that the type of work and their professional status falls within the conditions contained in Article 14(9) of the *Money Laundering Order*.

12. For example, the concession applies to litigation but not transactional work, so *Lawyers* should be mindful of the distinction between advice, litigation work and transactional work.

20.3 Risk Assessment

13. A *supervised person's* risk assessment is essential to directly inform and conduct the businesses approach to *AML/CFT/CPF*.

14. There are three levels to a lawyer's risk assessment:

- i) Business Risk Assessment (also known as Practice Wide Risk Assessments) to identify ML/TF/PF risks;
- ii) Customer Risk Assessments (client risk assessments) to identify the ML/TF/PF at individual *customer*/client level; and
- iii) Matter risk assessments on each new matter or a *customer*.

Those risks at ii) and iii) should feed back into the BRA.

15. Every *customer* has to have a risk assessment, and it may be possible to adopt a category-based approach to high/medium/low ratings (e.g. conveyancing matters of a value £3,000,000 or more are high risk). The following sub-sections set out some key legal service area vulnerabilities drawn from *FATF* and law enforcement guidance and case studies, and some key warning signs that have been drawn up by the Law Society for England and Wales, as an indication of service area vulnerabilities. Further factors to consider when evaluating the risks posed by *customers* and service areas are set out in section 3.3.4 of *this Handbook*.

20.3.1.1 Use of client accounts

Guidance notes

16. Lawyers should not provide a banking service for their *customer*s. However, it can be difficult to draw a distinction between holding *customer* money for a legitimate transaction and acting more like a bank. For example, when the proceeds of a sale are left with a *supervised person* to make payments, these payments may be to mainstream lending companies, but may also be to more obscure recipients, including private individuals, whose identity is difficult or impossible to check.

17. Situations which could give rise to cause for concern are detailed at section 6.7.2 of *this Handbook*.

18. *Supervised persons* should think carefully before disclosing client account details as this allows money to be deposited into a client account without the *supervised person's* knowledge. If it is necessary to provide account details, *supervised persons* should ask the *customer* where the funds will be coming from. Will it be an account in their name, from Jersey or another jurisdiction? *Supervised persons* should consider whether they are prepared to accept funds from any source that they are concerned about.

19. Circulation of client account details should be kept to a minimum. *Customers* should be discouraged from passing the details on to third parties and should be asked to use the account details only for previously agreed purposes.

20.3.1.2 Establish a policy on handling cash

Guidance notes

20. It is good practice to establish a policy of not accepting cash payments above a certain limit either at the *supervised person*'s office or into the *supervised person*'s bank account. Customers may attempt to circumvent such a policy by depositing cash directly into a client account at a bank. Supervised persons may consider advising *customer*s in such circumstances that they might encounter a delay in completion of the final transaction. Avoid disclosing client account details as far as possible and make it clear that electronic transfer of funds is expected.

20.3.1.3 *Source of funds*

Guidance notes

21. Accounts staff should monitor whether funds received from *customer*s are from credible sources. For example, it is reasonable for monies to be received from a company if your *customer* is a director of that company and has the authority to use company money for the transaction.

22. In some circumstances, cleared funds will be essential for transactions and *customers* may want to provide cash to meet a completion deadline. *Supervised persons* should assess the risk in these cases and ask more questions if necessary.

20.3.1.4 Private client work – Administration of estates

Guidance notes

23. A deceased person's estate is very unlikely to be actively utilised by criminals as a means for laundering their funds, however there is still a risk of *money laundering*, the *financing of terrorism*, or *proliferation financing* for those working in this area.

24. When winding up an estate, there is no blanket requirement that *supervised persons* should be satisfied about the history of all the funds which make up the estate under administration. However, *supervised persons* should be aware of the factors which can increase *money laundering, the financing of terrorism* or *proliferation financing* risks and consider the following:

- where estate assets have been earned in a foreign jurisdiction, *supervised persons* should be aware of the wide definition of criminal conduct in the *Proceeds of Crime Law*; and
- where estate assets have been earned or are located in a *higher risk country or territory*, *supervised persons* may need to make further checks about the source of those funds.

25. *Supervised persons* should be alert from the outset and monitor throughout so that any disclosure can be considered as soon as knowledge or suspicion is formed, and problems of delayed consent can be avoided (see section 9.4 of *this Handbook*).

26. *Supervised persons* should bear in mind that an estate may include criminal property. An extreme example would be where the *supervised person* knows or suspects that the deceased person was accused or convicted of acquisitive criminal conduct during their lifetime.

27. If *supervised persons* know or suspect that the deceased person improperly claimed welfare benefit/allowances or had evaded the due payment of tax during their lifetime, criminal property will be included in the estate and so a *money laundering* disclosure may be required.

28. Relevant local laws will apply before assets can be released. For example, a grant of probate will normally be required before UK assets can be released. *Supervised persons* should remain alert to warning signs, for example if the deceased or their business interests are based in a *higher risk country or territory*.

29. If the deceased person is from another jurisdiction and a *Lawyer* is dealing with the matter in the home country, *supervised persons* may find it helpful to ask the *Lawyer* for information about the deceased to gain some assurances that there are no suspicious circumstances surrounding the estate. The issue of the tax payable on the estate may depend on the jurisdiction concerned.

20.3.1.5 **Property transactions**

Guidance notes

30. Criminal conduct generates huge amounts of illicit capital, and these criminal proceeds need to be integrated into personal lifestyles and business operations. Law enforcement agencies have advised that property purchases are one of the most frequently identified methods of *money laundering*. Property can be used either as a vehicle for *money laundering* or as a means of investing laundered funds.

31. Criminals will buy property both for their own use, e.g., as principal residence or second homes, business, or warehouse premises, and as investment vehicles to provide additional income.

32. The purchase of real estate is commonly used as part of the last stage of *money laundering*. Such a purchase offers the criminal an investment which gives the appearance of financial stability. The purchase of a restaurant or hotel, for example, offers advantages as it is often a cash-intensive business, which is the preferred currency of criminals. Cash remains the mainstay of much serious organised criminal activity. It has the obvious advantage that it leaves no audit trail and is the most reliable form of payment, as well as the most flexible. Retail businesses also provide a good front for criminal funds where legitimate earnings can be mixed with the proceeds of crime.

20.3.1.6 **Criminal use of conveyancing services**

Guidance notes

33. Law enforcement agencies have advised that of all the services offered by Lawyers, conveyancing is the function most utilised by criminal groups. Conveyancing is a comparatively easy and efficient method of laundering money with relatively large amounts of criminal monies 'cleaned' in one transaction. In a stable or rising property market, the money launderer will incur no financial loss except fees. Conveyancing transactions can also be attractive to money launderers who are attempting to disguise the audit trail of the proceeds of their crimes. As the property itself can be 'criminal property' for the purposes of the Proceeds of Crime Law, Lawyers can still be involved in *money laundering* even if no money changes hands.

34. Corrupt *Lawyers* may employ trainees to perform the conveyancing work for criminal groups, thereby distancing themselves from the criminal aspect of the business. Conveyancers should also be alert to instructions which are a deliberate attempt to avoid assets being dealt with in the way intended by the court or through the usual legal process. For example, *Lawyers* may sometimes suspect that instructions are being given to avoid the property forming part of a bankruptcy or forming part of assets subject to confiscation.

20.3.1.7 **Ownership issues**

Guidance notes

35. Properties owned by nominee companies or multiple owners may be used as *money laundering* vehicles to disguise the true owner and/or confuse the audit trail. Supervised persons should be alert to sudden or unexplained changes in ownership.

36. Unexplained changes in ownership may indicate a form of *money laundering* known as "flipping", which involves a property purchase, often using someone else's identity. The property is then quickly sold for a much higher price to the same buyer using another identity. The proceeds of crime are mixed with mortgage funds for the purchase. This process may be repeated several times.

37. Another potential cause for concern is where a third party is providing the funding for a purchase, but the property is being registered in someone else's name. There may be legitimate reasons for this, such as a family arrangement, but *supervised persons* should be alert to the possibility of being misled about the true ownership of the property. Further *CDD* measures should be undertaken on the person providing the funding.

20.3.1.8 **Methods of funding**

Guidance notes

38. Many properties are bought with a combination of deposit, mortgage and/or equity from a current property. Usually, the Lawyer acting for the purchaser will have information about how the *customer* intends to fund the transaction. Lawyers should expect to be updated if those details change, for example, if a mortgage falls through and new funding is obtained.

39. *Supervised persons* should remember that payments made through the mainstream banking system are not guaranteed to be clean.

40. Transactions that do not involve a mortgage or are not being financed wholly from the sale of a previous property have a higher risk of being fraudulent. *Supervised persons* should be alert for large payments from such private sources of funds, especially if the *customer* receives payments from several individuals or sources. If concerns arise:

- the *customer* should be asked to explain the *source of funds*. *Supervised persons* should assess whether the explanation appears to be valid – e.g., the money has been received from an inheritance; and
- *supervised persons* should ensure that the *customer* is the *beneficial owner* of the funds being used in the purchase. Documentary evidence should be obtained in support of the same.

41. Settlements which are to be paid in cash – particularly where cash is to be passed directly between sellers and buyers without adequate explanation – may indicate *money laundering,* the *financing of terrorism,* or the *financing of proliferation*.

42. Third parties often assist with purchases and *supervised persons* may be asked to receive funds directly from third parties, for example relatives often assist first time buyers. Consideration will need to be given as to the extent of due diligence that needs to be undertaken on those third parties. *Supervised persons* should consider whether there are any obvious warning signs and what needs to be known about:

- the *customer*;
- the third party;
- their relationship; and
- the proportion of the funding being provided by the third party.

43. *Supervised persons* should consider their obligations to the mortgage lender in these circumstances – *supervised persons* are normally required to advise mortgage lenders if the buyers are not funding the balance of the price from their own resources.

20.3.1.9 Valuations

Guidance notes

44. An unusual sale price can be an indicator of *money laundering*. Whilst Lawyers acting in a property sale are not required to get independent valuations, if a *supervised person* becomes aware of a significant discrepancy between the sale price and what a property would reasonably be asked to sell for, consideration should be given to asking more questions.

45. Properties may also be sold below the market value to an associate, with a view to obscuring the title to the property while the original owner still maintains the *Beneficial ownership.*

20.3.1.10 Mortgage Fraud

Guidance notes

46. A *supervised person* may discover or suspect that a *customer* is attempting to mislead a lender to improperly inflate a mortgage advance – for example, by misrepresenting the borrower's income or because the seller and buyer are conspiring to overstate the sale price. Transactions which are not at arm's length may warrant particular consideration. However, until the improperly obtained mortgage advance is received, there is not any criminal property for the purposes of disclosure obligations to the FIU.

47. If a *supervised person* suspects that a *customer* is making a misrepresentation to a mortgage lender, the *supervised person* must either dissuade them from doing so or consider the ethical implications of continuing with the retainer. Even if a *supervised person* no longer acts for the *customer*, it may still be under a duty to advise the mortgage lender.

48. Large scale mortgage fraud is more sophisticated and will normally involve several properties. It may be committed by criminal groups or by individuals. The buy-to-let market is particularly vulnerable to large scale mortgage fraud, whether through new-build apartment complexes or large-scale renovation properties. Occasionally commercial properties will be involved.

49. Fraudsters may use private sources of funding such as property clubs, especially when credit market conditions tighten. These lenders often have lower safeguards than institutional lenders, leaving them vulnerable to organised fraud. Property clubs can be targeted particularly in relation to overseas properties where the property either does not exist, or is a vacant piece of land, not a developed property.

50. Sometimes fraud is achieved by selling the property between related private companies. The transactions will involve inflated values and will not be at arm's length. Increasingly, offshore companies are used with the property sold several times within the group before approaching a lender for a mortgage at an inflated value.

51. *Supervised persons* that discover or suspect that a mortgage advance has already been improperly obtained should consider advising the mortgage lender.

52. *Supervised persons* acting in connection with a re-mortgage who discover or suspect that a previous mortgage has been improperly obtained may need to advise the lender, especially if the re-mortgage is with the same lender. Consideration should also be given to making a disclosure to the *FIU* as the improperly obtained mortgage advance represents criminal property.

53. If a *customer* has made a deliberate misrepresentation on their mortgage application, it is likely that the crime/fraud exemption to legal professional privilege will apply (see section Legal Professional Privilege (LPP)20.5.1of *this Handbook*). This means that no waiver of confidentiality will be needed before a disclosure is made. However, such matters will need to be dealt with on a case-by-case basis.

20.3.1.11 Company and commercial work

Guidance notes

54. The nature of company structures can make them attractive to money launderers because it is possible to obscure true ownership and protect assets for relatively little expense. For this reason, Lawyers working with companies and in commercial transactions should remain alert throughout their business relationships, with existing as well as new *customer*s.

55. A common operating method amongst serious organised criminals is the use of front companies. These are often used to disguise criminal proceeds as representing the legitimate profits of fictitious business activities. They can also help to make the transportation of suspicious cargoes appear as genuine goods being traded. Often, they are used to mask the identity of the true *beneficial owners* and the source of criminally obtained assets. Corporate vehicles are also frequently used to help commit tax fraud, facilitate bribery/corruption, shield assets from creditors, facilitate fraud generally or circumvent disclosure requirements.

56. The lack of transparency concerning the *Beneficial ownership and control* of corporate vehicles has proved to be a consistent problem for *money laundering* investigations. Corporations acting as directors and nominee directors can be used to conceal the identity of the natural persons who manage and control a corporate vehicle.

57. Several international reports have highlighted the extent to which private limited companies, shell companies, bearer shares, nominees, front companies, and *SPVs* have been used in *money laundering* operations. Case studies submitted to the *FATF* have indicated the following common elements in the misuse of corporate vehicles:

- multi-jurisdictional and/or complex structures of corporate entities and trusts;
- foreign payments without a clear connection to the actual activities of the corporate entity;
- use of offshore bank accounts without clear economic necessity;
- use of nominees;
- use of shell companies;
- tax, financial and legal advisers were generally involved in developing and establishing the structure. In some case studies a *Lawyer* was involved who specialised in providing illicit services for *customers*.

58. The more of the above elements that exist, the greater the likelihood and the risk that the identity of the underlying *beneficial owner* may be able to remain unidentifiable.

20.3.1.12 Shell corporations

Guidance notes

59. The shell corporation is a tool that appears to be widely used by criminals. Often purchased "off-the-shelf", it can be a convenient vehicle for *money laundering* and for concealing the identity of the beneficial owner of the funds. The company records are often more difficult for law enforcement to access because they are held behind a veil of professional privilege or the professionals who run the company act on instructions remotely and anonymously.

60. Shell companies are often used to receive deposits of cash which are then transferred to another jurisdiction, to facilitate false invoicing or to purchase real estate and other assets. They have also been used as the vehicle for the actual predicate offence of bankruptcy fraud on many occasions.

20.3.1.13 Bearer shares

Guidance notes

61. Bearer shares confer rights of ownership to a company upon the physical holder of the share. They are commonly and legitimately used in several countries. However, the high level of anonymity that bearer shares offer provides opportunities for misuse where the identity of the shareholder is not recorded when the share is issued and transferred, ownership of the share is effectively anonymous.

62. Such shares are open to two *money laundering* risks:

- financial assets can be acquired without the purchaser being identified; and
- the company owners and controllers may not be capable of being identified.

63. To guard against misuse, several jurisdictions have dematerialised or immobilised bearer shares when they are registered in an effort to ensure that the identity of the *Beneficial owners* can be verified. Dematerialisation is achieved by requiring registration upon transfer or requiring registration to vote or collect dividends. While physical transfer of bearer shares is possible, it is believed to be rare.

20.3.1.14 Private equity

Guidance notes

64. Lawyers could be involved in any of the following circumstances:

- the start-up phase of a private equity business where individuals or companies seek to establish a private equity firm (and in certain cases, become authorised to conduct investment business);
- the formation of a private equity fund;
- ongoing legal issues relating to a private equity fund;
- execution of transactions on behalf of a member of a private equity firm's group of companies (a private equity sponsor that will normally involve a vehicle company acting on its behalf).

65. Private equity work may be considered to be low risk for *money laundering,* the *financing of terrorism,* or the *financing of proliferation* for the following reasons:

- private equity firms are also covered by the *Money Laundering Order* and similar legislation in equivalent jurisdictions;
- investors are generally large institutions, some of which will also be regulated for *money laundering* purposes;
- there are generally detailed due diligence processes followed prior to investors being accepted;
- the investment is generally illiquid, and the return of capital is unpredictable;
- the terms of the investment in the fund generally strictly control the transfer of interests and the return of funds to investors.

66. Factors which may alter this risk assessment include:

- where the private equity firm, fund manager or an investor is located in a jurisdiction which is not regulated for *money laundering* to a standard which is equivalent to the *FATF Recommendations;*
- where the investor is either an individual or an investment vehicle itself (a private equity fund of funds);
- where the private equity firm is seeking to raise funds for the first time or is approaching a large investor base.

20.3.1.15 Conveyancing transactions

Guidance notes

67. A *supervised person* may demonstrate that the basis upon which it has determined the value of a conveyancing transaction for the purposes of Article 4 of the *Money Laundering Order* is appropriate where it applies the value of the property that is the subject of the transaction.

20.4 Exemptions from *CDD* measures

Overview

68. This section is supplemental to and should be read in conjunction with section 8 of *this Handbook*.

69. Any relevant exemption as noted in (Section 8) may be applied. But also, Lawyer specific exemptions can be utilised if applicable:

Customer/Activity	Exemption	Article of MLO	Section of *this Handbook*	Conditions to be fulfilled before use?	Ongoing requirements?
Trust Customer	Third parties	17C(1) (c)(ii) and 17C(2)	8.2	Yes	Yes
Registered Property contracts passed before court	Customer	18(6)	8.3.7	Yes	Yes

20.4.1 Exemption from applying *third party identification requirements* in relation to certain *relevant customer*s involved in *Trust Company Business*

70. This section is supplemental to and should be read in conjunction with section 8.2 of *this Handbook*.

71. Article 17C(1)(c)(ii) of the *Money Laundering Order* provides that a *supervised person* that is a Lawyer is exempt from applying third party identification requirements in relation to a third party for which a relevant *customer* is acting if the relevant *customer* carries on Trust Company Business and is registered to carry on such business under the FS(J) Law, or equivalent business.

72. Article 17C(2) of the *Money Laundering Order* requires that a *supervised person* who does not apply *third party identification requirements* must be satisfied, by reason of the nature of the relationship with the *relevant customer*, that there is little risk of *money laundering, terrorism financing,* or *proliferation financing* occurring.

Guidance notes

73. In relation to the exemption set out at Article 17C(1)(c)(ii) of the *Money Laundering Order*, a *supervised person* may be satisfied that there is little risk of *money laundering,* the *financing of terrorism,* or the *financing of proliferation* occurring where:

- The service provided to a *Trust Company Business relevant customer* is drafting (including incidental reviewing and advising (insofar as the *Money Laundering Order* is applicable)) of one or more of the following and
- It considers the extent of the service provided.

In respect of trusts (except employee benefit schemes) administered by a *relevant customer* carrying on *Trust Company Business*, the service provided by the *supervised person* is drafting:

- a trust deed;
- a supplemental trust deed of:
  - appointment;
  - advancement;
  - disclaimer;
  - indemnity or release;
  - appointment, retirement and indemnity;
  - addition;
  - exclusion;

- amendment;
- change of proper law;
- revocation or termination.

› a loan agreement or loan assignment or novation;

› factual confirmations covering matters such as the existence and status of a trust and its trustee's capacity to enter into transactional documentation.

In respect of companies or partnerships administered by a *relevant customer* carrying on *Trust Company Business*, the service provided by the *supervised person* is drafting:

› incorporation documents;

› a loan agreement or loan assignment or novation;

› minutes and other corporate authorisations;

› stock transfer forms and share certificates;

› memoranda and articles of association;

› factual confirmations covering matters such as the existence and status of a company or partnership and its capacity to enter into transactional documentation.

In respect of employee benefit schemes (including pension schemes) controlled or administered by a *relevant customer* carrying on *Trust Company Business*, the service provided by the *supervised person* is drafting:

› a trust deed;

› a supplemental trust deed of:

- appointment;
- advancement;
- disclaimer;
- indemnity or release;
- appointment, retirement and indemnity;
- addition;
- exclusion;
- amendment;
- change of proper law;
- revocation or termination.

› a loan agreement or loan assignment or novation;

› factual confirmations covering matters such as the existence and status of a trust (or other vehicle by which the scheme is structured) and its capacity to enter into transactional documentation.

In respect of a foundation administered by a *relevant customer* carrying on *Trust Company Business*, the service provided by the *supervised person* is drafting:

› statutory forms;

› charters and regulations;

- supplemental deeds of:
    - initial and further endowments;
    - transfers of assets;
    - indemnities and releases;
    - distributions;
    - amendments and variations;
    - changes of proper law;
    - continuance and mergers, revocation, termination, winding up or dissolution;
    - appointment/removal of guardian or any other person appointed under the regulations of the foundation to carry out a function in respect of the foundation;
    - guardian sanctioning of council actions;
    - addition and removal of beneficiaries and changes of purposes;
    - addition, amendment, removal, exercise, assignment of founders' rights;
    - appointment and removal of council members;
    - releases of powers;
    - delegation of council powers.
- factual confirmations covering matters such as the existence and status of a foundation and its capacity to enter into transactional documentation.

74. The above is not intended to be an exhaustive list of documents for which drafting services are provided and a *supervised person* may be able to demonstrate that other drafting services present little risk of *money laundering*, *terrorist financing,* or *proliferation financing*.

75. A *supervised person* may demonstrate that it has considered the extent of the service provided to the *relevant customer* when it considers:

- whether the service provided is "off the shelf" or bespoke;
- the need for and extent to which an "off the shelf" service is to be modified; and
- the fee that is to be charged.

76. For example, the provision of a standard trust deed that requires very little modification, may be described as "off the shelf" and attracts only a nominal fee, may be illustrative of a relationship presenting little risk of *money laundering*. By contrast, the provision of a bespoke trust deed that requires detailed information on the trust to be collected and which attracts more than a nominal fee, may not.

20.4.2 Jersey property transfers

77. This section is supplemental to and should be read in conjunction with section 8.3.7 *of this Handbook*.

78. This section relates to the exemption available under Article 18(6) of the *Money Laundering Order*, which provides that a *supervised person* that is a *Lawyer* or a real estate agent, which enters into a *business relationship* or carries out a *one-off transaction* for the purpose of enabling a *customer*, directly or indirectly, to enter into a registered contract within the meaning of the Control of Housing and Work (Jersey) Law 2012 (i.e. where it is to be passed before the Royal Court and registered in the Public Registry of Contracts), need not obtain **evidence of identity** of its *customer*.

AML/CFT/CPF Codes of Practice

[COP178] For each case described in Article 18 of the *Money Laundering Order*, a *supervised person* must obtain information on the purpose and intended nature of the business relationship or one-off transaction.

[COP179] A *supervised person* that is a *lawyer* must obtain and retain documentation establishing that its *customer* is entitled to benefit from the exemption set out in Article 18(6) of the *Money Laundering Order*.

20.5 Reporting *money laundering* and *terrorist financing* activity

Overview

79. This section is supplemental to and should be read in conjunction with the *AML/CFT/CPF Codes of Practice* and *Guidance notes* set out at section 8 of *this Handbook*.

20.5.1 Legal Professional Privilege (LPP)

Overview

80. *Lawyers* are under a duty to keep the affairs of their *customers* confidential, and the circumstances in which they can disclose *customer* communications are strictly limited.

81. However, the *Proceeds of Crime Law* and *Terrorism Law* contain provisions requiring the disclosure of confidential information in certain circumstances to the police (or a *MLRO/Deputy MLRO*) by persons working in *supervised businesses*. These laws also provide individuals working for law firms which conduct *supervised business* with certain defences against proceedings for breaching any duty of confidentiality, or for an offence such as *money laundering*, if they make a disclosure to the police or to a *MLRO/Deputy MLRO* in accordance with the procedures set down by their employer.

82. This section examines some of the tensions which may arise between a *Lawyer*'s duty of confidentiality to their *customer* and the disclosure requirements set out in the *Proceeds of Crime Law* and *Terrorism Law*.

Statutory requirements (paraphrased wording)

83. *Article 34D of the Proceeds of Crime Law and Article 21 of the Terrorism Law contain comparable provisions. Those provisions provide that a person employed in a supervised business commits an offence if they come into possession of information in the course of that business which leads them to know or suspect, or have reasonable grounds to know or suspect, that another person is engaged in money laundering (e.g. the offences set out at Articles 30 and 31 of the Proceeds of Crime Law) or is committing an offence under Articles 15 and 16 of the Terrorism Law, or conduct outside Jersey which if occurring in Jersey would constitute one of the above offences. The offence is committed, unless the person reports their knowledge, suspicion or reasonable grounds to the FIU or to the MLRO (or Deputy MLRO) in accordance with their employer's procedures.*

84. *The Money Laundering Order requires that any person who conducts a financial services business in Jersey must have procedures in place for reporting such knowledge or suspicion to the FIU.*

85. *However, the Proceeds of Crime Law and Terrorism Law also include exemptions from the requirement to make such disclosures for professional legal advisers acting in privileged circumstances (see Article 34D(5) of the Proceeds of Crime Law, for example). Legal privilege is defined in the three laws referenced above. The exemptions do not apply to information or other matters communicated or given with a view to furthering a criminal purpose.*

86. *Article 35 of the Proceeds of Crime Law and Article 35 of the Terrorism Law prohibit disclosure of information in circumstances where a suspicious activity report has been made and/or where it would prejudice an existing or proposed investigation. However, an exception is also provided in respect of these offences where a professional legal adviser discloses any information or other matter:*

› *to a customer or to a representative of a customer of the legal adviser in connection with the giving of legal advice by the adviser to the customer; or*

› *to any person for the purpose of actual or contemplated legal proceedings.*

› *Again, this exemption does not apply in relation to any information or other matter that is disclosed with a view to furthering a criminal purpose.*

20.5.1.1 Duty of confidentiality

Overview

87. *Lawyers* are professionally and legally obliged to keep the affairs of their *customers* confidential. This obligation extends to all matters revealed to a *Lawyer*, from whatever source, by a *customer* or someone acting on the *customer's* behalf.

88. In exceptional circumstances, this obligation may be overridden. The most relevant instances are where a court orders disclosure or disclosure is required by statute.

20.5.1.2 Application of *LPP*

89. Certain confidential communications between a *Lawyer* and their *customer* will fall into a category known as *LPP*. *LPP* is a privilege against disclosure, ensuring *customers* know that certain documents and information provided to *Lawyers* cannot be disclosed without the *customer's* consent. It recognises a *customer's* right to be open with their legal adviser, without fear of later disclosure to their prejudice. *LPP* cannot be overridden by any other public interest but can be waived or overridden by statute.

90. *LPP* only covers those confidential communications falling under either **advice privilege** or **litigation privilege**. It does not cover all information/matters which *Lawyers* have a duty to keep confidential.

91. For the purposes of *LPP*, the term "*Lawyers*" includes Advocates, Écrivains, barristers, solicitors, in-house *Lawyers*, and their employees.

20.5.1.3 Advice Privilege

Guidance notes

92. Communications between a Lawyer and a *customer* are subject to **advice privilege** if:

- the *Lawyer* is communicating with the *customer* in their capacity as a *Lawyer*;
- the communications are confidential; and
- the communications are being made for the purpose of seeking advice from a lawyer or providing it to a *customer*.

93. Communications are not privileged simply because a *customer* is speaking or writing to their *Lawyer*. The protection applies only to those communications which directly seek or provide advice, or which are given in a legal context, that involve the *Lawyer* using their legal skills and which are directly related to the performance of the *Lawyer*'s professional duties.

94. Some examples of what is/is not covered by advice privilege, as established through case law, are set out below:

- communications **subject** to advice privilege:
    - a *Lawyer*'s bill of costs and statement of account;
    - information imparted by prospective *customers* in advance of a retainer, if the communications were made for the purpose of indicating the advice required.
- communications **not subject** to advice privilege:
    - notes of open court proceedings are not privileged as the content of the communication is not confidential;
    - a client account ledger maintained in relation to the *customer's* money;
    - an appointments diary or time record on an attendance note, time sheet or fee record relating to a *customer*;
    - conveyancing documents (these documents are not communicated and therefore are not subject to advice privilege).

20.5.1.4 Advice within a transaction

95. All communications between a *Lawyer* and their *customer* relating to a **transaction** in which the *Lawyer* has been instructed for the purpose of obtaining legal advice are covered by advice privilege, provided that they are directly related to the performance by the *Lawyer* of their professional duty as legal adviser of their *customer*.

96. This means that where a *Lawyer* is providing legal advice in a transactional matter (such as conveyancing) the advice privilege will cover all:

- communications with;
- instructions from; and
- advice given to;

The *customer*, including any working papers and drafts prepared, as long as they are directly related to the *Lawyer*'s performance of their professional duties as a legal adviser.

20.5.1.5 ***Litigation Privilege***

Guidance notes

97. **Litigation privilege** is wider than advice privilege and protects confidential communications made in pursuance or contemplation of litigation, between either:

- a Lawyer and a *customer*;
- a Lawyer and an agent, whether or not that agent is a Lawyer; or
- a Lawyer and a third party.

98. Such communications must be for the sole or dominant purpose of litigation, namely:

- for seeking or giving advice in relation to it;
- for obtaining evidence to be used in it; or
- for obtaining information leading to obtaining such evidence.

20.5.1.6 **What is covered by *LPP* – Further points to consider**

99. An original document not brought into existence for privileged purposes, and thus not already privileged, does not become privileged simply by being given to a *Lawyer* for advice or another privileged purpose.

100. Furthermore, where a *Lawyer* has a *customer* which is a body corporate, communication between the *Lawyer* and the employees of the corporate *customer* may not be protected by *LPP* if those employees are not considered to be the *customer* for the purpose of the retainer. As such, some employees will be *customers*, while others will not.

101. It is not a breach of *LPP* to discuss a matter with your *MLRO* (or *Deputy MLRO*) for the purpose of receiving guidance on whether to make a disclosure. Privilege will continue to apply whilst such a determination is being made.

20.5.1.7 **Crime/Fraud Exception**

Guidance notes

102. LPP protects advice a Lawyer gives to a *customer* on avoiding committing a crime or warning them that proposed actions could attract prosecution. LPP **does not extend** to documents which themselves form part of a criminal or fraudulent act, or communications which take place in order to obtain advice with the intention of carrying out an offence. It is irrelevant whether or not the Lawyer is aware that they are being used for that purpose.

103. Article 32 of the *Proceeds of Crime Law* and Article 22 of the *Terrorism Law* provide that, if a *Lawyer* discloses information under those laws, the disclosure will not be treated as a breach of any restriction on disclosure contained in any statute, contract or otherwise.

104. It is not just a ***customer's*** intention which is relevant for ascertaining whether information was communicated for the furtherance of a criminal purpose. In addition to the circumstances described above, *LPP* **also does not extend** to a situation where a **third party** intends the *Lawyer-customer* communication to be made for the furtherance of a criminal purpose (e.g., the innocent *customer* is being used by a criminal third party).

20.5.1.8 Determining when to submit a *SAR*

105. The reporting obligations and offences contained in Article 34D of the Proceeds of Crime Law and Article 21 of the *Terrorism Law* do not apply to a *Lawyer's* knowledge or suspicion, or reasonable grounds for knowledge or suspicion, arising from information obtained in "privileged circumstances" (as defined by the above laws). The *Money Laundering Order* also makes a provision in respect of privileged circumstances at Article 21(5). A *Lawyer* may, however, wish to consider making a joint report with their *customer*. The agreement of the *Lawyer*'s *customer* to waive *LPP* is necessary for this to be possible.

106. If information leading to knowledge, suspicion or reasonable grounds for knowledge or suspicion is obtained in circumstances that are not covered by *LPP*, a disclosure should be made to avoid the commission of an offence of failing to disclose. *Lawyers* will not be in breach of their professional duty of confidentiality if they make a report in these circumstances.

107. If a *Lawyer* commits an offence under Article 30 of the *Proceeds of Crime Law* or Article 16 of the *Terrorism Law* they should make a disclosure to the FIU or their *MLRO*/*Deputy MLRO*, otherwise they will not be able to avail themselves to the defences which operate under those Articles.

108. As the application of *LPP* is complex, *supervised persons* carrying on legal business may wish to consider maintaining procedures which require reports to be made to the *MLRO* (or *Deputy MLRO*) **on each occasion** that there is knowledge, suspicion, or reasonable grounds to suspect *money laundering* or the *financing of terrorism*. The *MLRO* (or *Deputy MLRO*) can then discuss the situation with the employee concerned and, as necessary, take advice from an appropriate partner.

20.5.1.9 *CDD* measures and *LPP*

Guidance notes

109. To assist in complying with the requirements of the Proceeds of Crime Law, *supervised persons* carrying on legal business may wish to consider separating all material on *customer* files so that it is clear what material is non-privileged and what material is covered by LPP.

110. *CDD* and risk assessment documents should be completed, where possible, in a way which distinguishes privileged and non-privileged information. *Supervised persons* carrying on legal business may wish to consider including guidance to this effect in their procedures. This will assist in ensuring that the *JFSC* can request information from and conduct examinations of *supervised persons* with the minimum disruption to business, thus aiding in the *supervised person's* compliance with their obligations to the *JFSC*.

21 *ACCOUNTANTS*

21.1 Definition and overview of *Accountants* undertaking *supervised business*

1. Paragraph 22 of Part 3 of Schedule 2 to the *Proceeds of Crime Law* defines the relevant operations and activities of *Accountant*s for the purposes of complying with *AML* requirements in the *Money Laundering Order*. *Guidelines* provide interpretation and the activities and operations of *Accountant*s that are in scope.

21.1.1 Activities to which the *Money Laundering Order* applies

Overview

2. For the purposes of *this Handbook*, "*accountancy services"* is limited to those services set out in the *Guidelines.*

3. Where the services provided by an *Accountant* do not fall within the definition of accountancy services, all persons and businesses within Jersey are covered by the primary legislation covering *money laundering*, the *financing of terrorism*, or the *financing of proliferation*.

4. *Accountant*s involved in the provision of management consultancy or interim management should be alert to the possibility that they could fall within the scope of the *Money Laundering Order* and by extension *this Handbook* to the extent that they provide any supervised business when acting under a contract for services in the course of business.

21.1.2 Tax advisers

Overview

5. Refer to the Glossary of *this Handbook* for *this Handbook's* definition of *tax advisers*, and the *Guidelines* for a description of particular services that fall within Schedule 2 of the *Proceeds of Crime Law.*

6. A *tax adviser* should be aware of the *JFSC's* responsibility to regulate *Trust and Company Business*, which may impinge upon the work *tax advisers* undertake for their *customers*.

7. Whilst *tax advisers* are more likely to identify tax offences, they need to be aware of the potential requirement to report knowledge or suspicion of proceeds derived from any criminal conduct (as defined in Article 1 of the *Proceeds of Crime Law*) which is encountered in the course of business as a *tax adviser*.

21.1.3 Audit services

Overview

8. Refer to the Glossary of *this Handbook* for a definition of *audit services*, and *the Guidelines* for a description of particular services that fall within Schedule 2.

9. The extent to which the *Anti-Money Laundering and Counter-Terrorism Legislation* affects the auditor's work differs between two broad categories of audit – audits of *supervised persons* and audits of other types of entity.

21.1.3.1 Audits of *supervised persons*

Guidance notes

10. *Supervised persons* carrying on *supervised business* are required to comply with the *Money Laundering Order* which places obligations on them to combat *money laundering,* the *financing of terrorism*, or the *financing of proliferation*. All such businesses are required to comply with the *AML/CFT/CPF Codes of Practice* and *Guidance notes* issued by the *JFSC* (see section 2.6 of *this Handbook*, which covers the monitoring of compliance with the same).

11. In addition to reporting on their financial statements, auditors of such businesses are required to report to the *JFSC* on matters of significance that come to their attention in the course of their work. This includes non-compliance with legislation, departures from its requirements and suspicions that the directors and management of such entities are implicated in *money laundering* (see section 9 of *this Handbook*). Therefore, auditors of such businesses should not only be aware of the key provisions contained in the *Money Laundering Order* as they affect auditors themselves, but also the requirements of the wider *AML/CFT/CPF Handbook*, including any sector-specific AML/CFT/CPF Codes of Practice and Guidance notes relevant to the business that they are auditing.

21.1.3.2 Audits of other types of entity

Guidance notes

12. In general, auditors of other types of entity not covered by the *Money Laundering Order* are required only to take appropriate steps in response to factors encountered in the course of their work which led them to suspect that *money laundering,* the *financing of terrorism,* or the *financing of proliferation* is taking place.

21.1.3.3 Detection of *money laundering*, the *financing of terrorism*, and the *financing of proliferation*

Guidance notes

13. Whilst auditors have no statutory responsibility to undertake work solely for the purpose of detecting *money laundering,* the *financing of terrorism,* and/or the *financing of proliferation*, they nevertheless need to take the possibility of *money laundering,* the *financing of terrorism*, and the *financing of proliferation* into account in the course of carrying out procedures relating to fraud and compliance with the *Anti-Money Laundering and Counter-Terrorism Legislation*. An auditor's wide access to documents and systems, and the need to understand the business, can make them ideally suited to spot such issues as they arise.

14. However, auditors cannot be held responsible for the prevention of, and failure to detect, the *financing of terrorism,* or the *financing of proliferation* activities in the entities they audit. External auditors performing financial statement audits within a short timescale may be less likely than other professional *Accountants* (such as forensic *Accountants* and *Accountants* in management positions) to encounter signs of possible *money laundering,* the *financing of terrorism,* or the *financing of proliferation*. Nor is it the auditors' responsibility to detect suspicious activity in connection with a compliance or operational audit of an *AML/CFT/CPF programme* or testing a *SAR* process.

21.1.4 Insolvency services

Overview

15. The terms insolvency services and insolvency practitioners are defined in the Glossary of *this Handbook*. *The Guidelines* further describe particular insolvency services that fall within Schedule 2 of the *Proceeds of Crime Law*.

21.1.5 Accountants undertaking supervised business

Overview

16. *The Guidelines* indicate that accountancy businesses may provide other services that fall within the scope of Schedule 2 of the *Proceeds of Crime Law*. These include:

- undertaking investment related activity, including acting as a financial intermediary;
- advising on the setting up of trusts, companies or other bodies;
- acting as trustee, nominee or company director;
- giving advice on capital structures, acquisitions and securities issues;
- providing safe custody services;
- arranging loans.

17. Consequently, some *supervised persons* providing *accountancy services* are authorised and regulated by the *JFSC* under the *FS(J) Law* and subject to one or more of the Investment Business, *Trust Company Business* and Funds Services Business *Codes of Practice*. *Supervised persons* who are so regulated should therefore have regard to any relevant sector-specific sections of *this Handbook* when drawing up their *policies and procedures* for the prevention and detection of *money laundering*, the countering of *terrorist financing*, and the countering of *proliferation financing* in respect of those regulated activities.

21.2 Risk-based approach to *identification measures*

Overview

18. This section must be read in conjunction with, and is supplemental to, the *Guidance notes* set out at section 3.3.2 of *this Handbook* (Information for Assessing Risk – Stage 1.4).

19. The *Guidance notes* set out below provide sector-specific guidance on additional factors *supervised persons* providing *accountancy services* may need to consider, to appropriately assess the risk that a *business relationship* or *one-off transaction* will involve *money laundering*, the *financing of terrorism*, or the *financing of proliferation*.

21.2.1.1 Insolvency cases

Guidance notes

20. In the context of insolvency work, the *customer* is considered to be the insolvent. An *insolvency practitioner* should risk assess, identify and verify the *customer* over which they are appointed.

21. A situation where an *insolvency practitioner* is required may be urgent, for example, if there is a risk of dissipation of assets and erosion of value. It is therefore important for an *insolvency practitioner* to be certain about the identity of the *customer* over which they are taking appointment.

21.2.1.2 Auditing standards on acceptance of client relationships

Guidance notes

22. Auditing standards on quality control for audits state that acceptance of *business relationships* and specific audit engagements includes considering the integrity of the principal owners, key management and those charged with governance of the *customer*. This involves the auditor making appropriate enquiries and may involve discussions with third parties, the obtaining of written references and searches of relevant databases.

23. The extent of knowledge a *supervised person* providing *audit services* will have regarding the integrity of a *customer* will generally grow within the context of an ongoing *business relationship* with that *customer*. However, useful information may be obtained at the outset of a *business relationship* including, for example:

- the reasons for the proposed appointment of the *supervised person* and non-reappointment of the previous auditors;
- communications with existing or previous providers of professional accountancy, banking and legal services to the *customer*; and
- background searches and the review of relevant databases.

24. Whilst adherence to auditing standards may provide some relevant *customer* identification information, they will not be sufficient on their own to comply with the requirements of the *Money Laundering Order* and *this Handbook*.

21.3 *Identification measures*

21.3.1 Obligation to find out identity and obtain evidence: Individuals

Overview

25. This sector-specific section is supplementary to and should be read in conjunction with section 4.2.1 of *this Handbook*.

21.3.1.1 Insolvency cases

26. It may not always be possible or necessary to obtain identification evidence direct from individuals, individual shareholders or directors in respect of an insolvent company as their co-operation may not be forthcoming.

Guidance notes

27. An insolvency practitioner may demonstrate compliance with Article 3 of the *Money Laundering Order* where it obtains evidence of the identity of the person or entity over which they are appointed. Acceptable evidence may include a court order, a court endorsed appointment, or an appointment made by a debenture holder or creditors meeting supported by a company search or similar.

21.3.2 Urgent undertakings

28. Section 4.7 of *this Handbook* sets out statutory requirements under the *Money Laundering Order* regarding when identification measures must be applied, in respect of a business relationship or one-off transaction.

29. Where the provision of supervised business by the *Accountant* is urgent, this undertaking may be provided prior to obtaining evidence of identity if there is little risk of *money laundering*, the *financing of terrorism*, or the *financing of proliferation* occurring, and *evidence of identity* is obtained as soon as reasonably practicable.

21.3.3 Ascertaining legal position

Overview

30. Section 4.8 of *this Handbook* sets out the statutory requirements under the *Money Laundering Order* to terminate a *business relationship* or not carry out a *one-off transaction* where a *supervised person* is unable to apply *identification measures* in respect of that relationship or *one-off transaction*.

31. A concession from terminating a *business relationship* is permitted for *Accountants*, *Lawyers* and other professional advisers who are in the course of ascertaining the legal position for their *customer* or performing the task of defending or representing their *customer* in legal proceedings (including advice on instigating or avoiding proceedings).

32. To qualify for the concession the *Accountant*, *Lawyer* or other professional adviser must be a member of a supervised professional body that undertakes competency testing for its members and imposes and maintains professional and ethical standards.

Statutory requirements (paraphrased wording)

33. Article 14(9) of the *Money Laundering Order* provides that the prohibition from continuing a *business relationship* does not apply where the relevant person is a *Lawyer* or other business falling within paragraph 21 or 22 of Part 3 of Schedule 2 to the *Proceeds of Crime Law* and is in the course of ascertaining the legal position for that person's client or performing the task of defending or representing the client in, or concerning legal proceedings, including advice on instituting or avoiding proceedings.

Guidance notes

34. *CDD* information will still need to be collected within a reasonable timescale to comply with Article 13 of the *Money Laundering Order*.

35. *Accountants*, *Lawyers*, and other supervised professional advisers are encouraged to consider their position very carefully before applying this concession to ensure that the type of work and their professional status falls within the conditions contained in Article 14(9) of the *Money Laundering Order*.

21.3.4 Exemptions from *CDD* Measures

Overview

36. This section is supplemental to and should be read in conjunction with section 8.2 of *this Handbook*.

37. Accountant relevant exemptions:

Customer/Activity	Exemption	Article of MLO	Section of *this Handbook*	Conditions to be fulfilled before use?	Ongoing requirements?
Trust Customer	Third parties	17C(1) (c)(ii) and 17C(2)	8.2	Yes	Yes

38. Article 17C(1)(c)(iii) of the *Money Laundering Order* provides that a *supervised person* that is an Accountant is exempt from applying third party identification requirements in relation to a third party for which a relevant *customer* is acting if the relevant *customer* carries on Trust Company Business and is registered to carry on such business under the FS(J) Law, or equivalent business.

39. Article 17C(2) of the *Money Laundering Order* requires that a *supervised person* who does not apply third party identification requirements must be satisfied, by reason of the nature of the relationship with the relevant *customer*, that there is little risk of *money laundering*, *terrorist financing*, or *proliferation financing* occurring.

Guidance notes

40. In relation to the exemption set out at Article 17C(1)(c)(iii) of the *Money Laundering Order*, a *supervised person* may demonstrate that due to the nature of the relationship with the relevant *customer*, there is little risk of *money laundering*, the *financing of terrorism*, or the financing of proliferation occurring where the service being provided to the relevant *customer* is the provision of:

› generic information on Jersey accounting requirements for the preparation of financial statements; or

› generic information on Jersey tax requirements; and

› it considers the extent of the service provided.

41. A *supervised person* may demonstrate that it has considered the extent of the service provided when it considers:

› the extent of any further explanation of the Jersey accounting or tax requirements that may subsequently be needed; and

› the fee that is to be charged.

42. For example, the provision of generic information on Jersey accounting or tax requirements that requires no more than an explanation of a Jersey accounting or tax requirement and attracts only a nominal fee, may be illustrative of a service which presents little risk of *money laundering*, terrorism financing, or *proliferation financing*. By contrast, the provision of detailed and complex tax structuring services that require detailed information of the person or arrangement in question to be collected and attracts more than a nominal fee, may indicate a higher risk of *money laundering*.

21.4 *Business Risk Assessment*

21.4.1 Considering *customer* and service risks to the business

Overview

43. Further factors to consider when evaluating the risks posed by *customer*s and service areas are set out in section 3.3.4 of *this Handbook*.

21.4.1.1 Accountancy, audit and *insolvency services* risk

Guidance notes

44. Those providing *accountancy services*, *audit services* or *insolvency services* will primarily need to consider their *BRA* in respect of the nature of their *customer* base, the business sectors in which their *customers* operate and the geographical location of their *customers*. The standing of *customers* and adherence to sound corporate governance principles will also have an impact including those *customers* that have previously been prosecuted or fined for criminal or regulatory offences.

45. The *BRA* should take account of the following risks:

- setting up, winding up, or effecting recovery for high cash turnover businesses for *customers* which may provide a front for criminal money;
- being used in an active sense to launder money through the handling of cash or assets or through payments that are made to, or received from, third parties, particularly with a cross-border element;
- becoming concerned in an arrangement which facilitates *money laundering* through the provision of investment services;
- becoming a party to serious fraud on the part of senior management or failing to recognise the warning signs relating to management fraud; and
- the potential for *money laundering,* the *financing of terrorism,* and the *financing of proliferation* to become attached to the *customer* and/or those who trade with or otherwise interact with *customers*.
- those providing *accountancy services* should also consider the risks when:
    - providing assistance in setting up trusts or company structures which could be used to obscure beneficial ownership of monies and assets settled into trust; and
    - handling the financial affairs, or setting up companies, trusts or other structures for politically exposed persons whose assets and wealth may be derived from the proceeds of corruption (see section 7.6 of *this Handbook*).

21.4.1.2 Taxation service risk

Guidance notes

46. *Tax advisers* are not required to be experts in criminal law, but they are expected to be aware of the offences which can give rise to the proceeds of crime. For example, *tax advisers* should be aware of the boundaries between deliberate understatement or other tax evasion and simple cases of error or genuine differences in the interpretation of tax law. The main areas where offences may arise which might increase the risks of the *tax adviser* becoming concerned during an engagement are (note the below list is not exhaustive):

- tax evasion, including making false returns (including supporting documents), accounts or financial statements or deliberate failure to submit returns;
- deliberate refusal to correct known errors;
- fraudulent or dishonest conduct;
- fraudulent evasion of *VAT* by *customers* operating within the *EU* including the possession and dealing in goods on which *VAT* has been evaded (e.g., missing trader intra community/carousel fraud).

21.5 *Money laundering, terrorist financing* and *proliferation financing* warning signs for accountancy sector

Overview

47. This section must be read in conjunction with, and is supplemental to, the warning signs set out at section 6.7 of *this Handbook*.

48. Article 13 of the *Money Laundering Order* requires a *supervised person* to apply ongoing monitoring throughout the course of a *business relationship* and take steps to be aware of transactions with heightened *money laundering, the financing of terrorism,* or the *financing of proliferation* risks. The *Proceeds of Crime Law* requires a *supervised person* to report suspicious transactions and activity (see section 8 of *this Handbook*).

49. This section highlights several warning signs for *supervised persons* providing *accountancy services* to help them decide whether there may be reasons for concern or the basis for a reportable suspicion.

50. *Supervised persons* providing *accountancy services* should have regard both to the sector-specific warning signs set out below and the general indicators described at section 6.4 of *this Handbook*, where they may become vulnerable to *money laundering,* the *financing of terrorism,* or the *financing of proliferation*. These warning signs apply both to circumstances that may arise at the start of a *business relationship* and to those arising during ongoing monitoring.

51. Because money launderers, terrorist financers and proliferators are always developing new techniques, no list of examples can be fully comprehensive. However, the following are some key factors indicating activity or transactions which might heighten a *customer's* risk profile or give cause for concern.

21.5.1 Accountancy and audit services

52. Any of the following general warning signs should prompt additional questions or investigation by those offering *accountancy services* and *audit services*:

- use of many different firms of auditors and advisers for connected companies and businesses;
- the client has a history of changing bookkeepers or *Accountant*s yearly;
- company records consistently reflect sales at less than cost, thus putting the company into a loss position, but the company continues to operate without reasonable explanation of the continued loss.

21.5.2 Tax advisers

53. There are several tax offences which can give rise to the proceeds of crime and therefore require the submission of a *SAR* to the *FIU*. A *tax adviser* is not required to be an expert in criminal law, but they would be expected to be aware of the boundaries between deliberate understatement or other tax evasion and simple cases of error or genuine differences in the interpretation of tax law and be able to identify conduct in relation to direct and indirect taxation which is punishable by the criminal law.

54. There will, however, be no question of criminality where the *customer* has adopted in good faith, honestly and without misstatement, a technical position with which a revenue authority disagrees.

55. The main areas where offences may arise in relation to direct taxation are:

- tax evasion, including making false returns (including supporting documents), accounts or financial statements or deliberate failure to submit returns; and
- deliberate refusal to correct known errors.

21.5.2.1 Innocent or negligent error

56. It is not uncommon for *tax advisers* to become aware of errors or omissions, in current or past years, from *customer's* tax returns, or any calculations or statements appertaining to any liability, or an underpayment of tax, for example, because a payment date has been missed. If the *tax adviser* has no cause to doubt that these came about because of an innocent mistake or negligence, then they will not have formed a suspicion. However, in some cases the *tax adviser* may form a suspicion that the original irregularity was criminal in nature, and this will then become a reportable suspicion.

21.5.2.2 Unwillingness or refusal to disclose to a revenue authority

57. Where a *customer* indicates that they are unwilling, or refuse, to disclose the matter to a revenue authority (e.g., HMRC, Revenue Jersey etc) to avoid paying the tax due, the *customer* appears to have formed a criminal intent and therefore a reporting obligation arises. The *tax adviser* should also consider whether they can continue to act and should consult their professional body's guidance on such matters. This paragraph applies equally to potential *customers* for whom the *tax adviser* has declined to act.

21.5.2.3 Adjusting subsequent returns

58. Where the legislation permits the correction of small errors by subsequent tax adjustments, and the original error was not attributable to any criminal conduct, then the adjustment itself will not give rise to the need to report, since no crime will have been committed.

21.5.2.4 Intention to underpay

59. A *customer* may suggest that they will, in the future, underpay tax. This would be tax evasion and a *money laundering* offence when it occurs. A *tax advisor* can and should apply their professional body's normal ethical guidance to persuade the *customer* to comply with the legislation. Should the *customer's* intention in this regard remain in doubt, the *tax adviser* should consider carefully whether they can commence or continue to act, and if in doubt should seek specialist legal advice. A *SAR* may well be required in such cases.

21.5.2.5 Offences applicable to Value Added Tax

60. A *customer* which is a business resident in the *UK* or an *EU* member state will normally be subject to *VAT*. Guidance on the offences applicable to *VAT*, for example fraudulent evasion of *VAT* and production or sending of false documents or statements, is set out in the 'Supplementary Anti *Money Laundering* Guidance for Tax Practitioners' produced as an appendix to the AML/CFT Guidance for the Accountancy Sector released by the UK Consultative Committee of Accountancy Bodies (**CCAB**).

21.5.3 Business recovery or receiverships

61. *Insolvency practitioners* will often encounter criminal activity when winding up or effecting recovery for a business. Serious fraud which has resulted in benefit either for the business or an individual will be reportable to the *FIU* as will incidences where the business has been used to launder the proceeds of crime. Examples may be where:

- fraud has caused or contributed to the failure of the business;
- there has been illegal siphoning off or transfer of assets by directors/shareholders;
- false accounting or misrepresentation of profits has been applied to maintain share value;
- the directors or members of senior management have been guilty of illegal trading or market abuse;
- tax fraud has been committed by reducing income or profits; or
- a white knight (a form of hostile takeover defence by a 'friendly' buyer) has invested criminal funds.

21.5.3.1 Observation of unlawful conduct resulting in advice

62. It should be borne in mind that for property to be criminal property, not only must it constitute a person's benefit from criminal conduct, but the alleged offender must know or suspect that the property constitutes such a benefit. This means, for example, that if someone has made an innocent error, even if such an error resulted in benefit and constituted a strict liability criminal offence, then the proceeds are not criminal property, and no *money laundering* offence has arisen until the offender becomes aware of the error.

63. Examples of unlawful behaviour which may be observed, and may well result in advice to a *customer* to correct an issue, but which are not reportable as *money laundering*, are set out below:

- offences where no proceeds or benefit results, such as the late filing of company accounts. However, *supervised persons* should be alert to the possibility that persistent failure to file accounts could represent part of a larger offence with proceeds, such as fraudulent trading or credit fraud involving the concealment of a poor financial position;
- misstatements in tax returns, for whatever cause, but which are corrected before the date when the tax becomes due;
- attempted fraud where the attempt has failed and so no benefit has accrued (although this may still be an offence in some jurisdictions e.g., the UK); and
- where a *customer* refuses to correct, or unreasonably delays in correcting, an innocent error that gave rise to proceeds and which was unlawful, firms should consider what that indicates about the client's intent and whether the property has now become criminal property.

21.6 Reporting *money laundering* and *terrorist financing* activity

21.6.1 Further enquiries by auditors

Overview

64. This section is supplemental to and should be read in conjunction with section 8.2 of *this Handbook* (Reporting knowledge or suspicion).

65. Section 8.2 *of this Handbook* states that there is a reporting requirement under Article 34D of the *Proceeds of Crime Law* and Article 21 of the *Terrorism Law* to make a *SAR* when there is knowledge, suspicion or reasonable grounds for suspecting that:

- another person is engaged in *money laundering* or the *financing of terrorism*; or
- any property constitutes or represents proceeds of criminal conduct; or
- any property has been, is being or is intended to be used in criminal conduct; or
- any property is or may be terrorist property.

66. Once an auditor suspects a possible breach of legislation which may require a report under the laws referenced above, further enquiries will need to be made. Auditing standards require that when the auditor becomes aware of information concerning a possible breach, the auditor should obtain an understanding of the nature of the act and the circumstances in which it has occurred. Sufficient information should be obtained to evaluate the possible effect on the *customer's* financial statements.

67. However, the *Anti-Money Laundering and Counter-Terrorism Legislation* does not require an auditor to undertake any additional enquiries to determine further details of the predicate criminal offence (i.e., the offence giving rise to the proceeds of crime). To help mitigate the risk of tipping-off, it is important that any further enquiries only represent steps that the auditor would have performed as part of the normal audit work and that the *MLRO* (or *Deputy MLRO*) is consulted before any further enquiry is performed. If an employee of the auditor is genuinely uncertain as to whether there are grounds to make a *SAR*, they may wish to seek advice from their *MLRO* (or *Deputy MLRO*).

68. During the course of the audit work, the auditor might obtain knowledge or form a suspicion about a proposed act that would be a criminal offence but has yet to occur. Because attempting or conspiring to commit a *money laundering* offence is itself a criminal act, a *SAR* may need to be made in some circumstances.

69. Where the auditor makes an internal *SAR* to the *MLRO* (or *Deputy MLRO*) and it is decided that further enquiry is necessary, the *auditor* will need to be made aware of the outcome of the enquiry to determine whether there are any implications for the audit report or the decision to accept reappointment as auditor.

70. The auditor will need to consider whether continuing to act for the *customer* could itself constitute a *money laundering offence*. For example, if it amounted to aiding or abetting the commission of one of the principal *money laundering* offences such as becoming involved in an arrangement. In those circumstances the auditor may wish to consider resigning but should first contact their *MLRO* (or *Deputy MLRO*) to report the suspicion and seek guidance in respect of tipping-off. If the auditor wishes to continue to conduct the audit, appropriate consent may be required from the *FIU*.

71. Partners and employees of *supervised persons* carrying on *audit services* will need to follow their internal reporting procedures when considering whether to include documentation relating to *money laundering* reporting in the audit working papers.

21.6.2 Auditor's responsibility for monitoring compliance

Overview

72. The International Standard on Auditing's Policy Paper ISA 250 establishes standards and provides guidance on the auditor's **responsibility to consider legislation** in an audit of financial statements. The *Anti-Money Laundering and Counter-Terrorism Legislation* does not require the auditor to extend the scope of an audit except as set out in section 16.7.3 of *this Handbook*, but regular audit work could still give rise to knowledge or suspicion, or reasonable grounds for knowledge or suspicion, that will need to be reported. Such knowledge or suspicion may arise in relation to:

› legislation linked directly to the preparation of the financial statements;

› legislation which provides a legal framework within which the *customer* conducts its business; and

› other legislation.

73. Auditing standards relating to legislation require the auditor to obtain sufficient appropriate audit evidence regarding **compliance** with the legislation that has an effect on the determination of material amounts and disclosures in the financial statements. This may result in the auditor becoming suspicious that, for example, fraud or tax offences have taken place, which may be criminal offences resulting in the acquisition of criminal property.

74. Auditing standards on legislation also require the auditor to carry out procedures to help identify possible or actual instances of **non-compliance** with the legislation which provides a legal framework within which the *customer* conducts its business and is therefore central to its financial statements. These procedures involve:

› obtaining a general understanding of the legal and regulatory framework applicable to the *customer* and its wider industry, and of the procedures followed to ensure compliance with that framework;

› inspecting correspondence with the relevant licensing and regulatory authorities;

› making enquiries to the Board/senior management of the *customer* as to whether they are on notice of any such possible instances of **non-compliance** with those laws or regulations; and,

› obtaining written representation that the Board/senior management have disclosed to the auditor all known actual or possible instances of **non-compliance** with legislation whose effects should be considered when preparing financial statements, together with - where applicable - the actual or contingent consequences which may arise from the **non-compliance** (i.e., regulatory fines, public censure etc).

75. This work may give the auditor grounds to suspect that criminal offences have been committed, and which may need to be reported to the *FIU*.

76. If the *customer* falls within the definition of a *financial services business*, legislation relating to *money laundering* will be central to the operation of their business. When auditing the financial statements of such *customers*, the auditor must review the steps taken by the *customer* to comply with the *Money Laundering Order* and the *JFSC's* other regulatory requirements, assess their effectiveness and obtain board/senior management representations concerning compliance with them. If the *customer's systems and controls* (including *policies and procedures*) appear to be ineffective, the auditor must consider whether there is an obligation to report a matter of "material significance" to the *JFSC* and the possible impact of any regulatory action which may arise from the same (see section 16.7.3 of *this Handbook* for further information).

77. The *auditor* will need to consider whether any **contingent liabilities** may arise in this area. For example, there may be criminal fines for **non-compliance** with the *Anti-Money Laundering and Counter-Terrorism Legislation*. In certain circumstances, civil claims or confiscation proceedings may occur, giving rise to contingent liabilities. The *auditor* will also need to remain alert to the fact that discussions with the *customer* on such matters may create a risk of tipping off (see section 8.5 of *this Handbook*).

78. In some situations, the *auditor's customer* may have obtained legal advice to the effect that certain actions or circumstances do not give rise to criminal conduct and therefore cannot give rise to criminal property. Determining whether an act constitutes **non-compliance** with the *Anti-Money Laundering and Counter-Terrorism Legislation* may involve consideration of matters which do not lie within the competence and experience of the *auditor*. As a result, provided that the *auditor* considers that the advice has been obtained from a suitably qualified and independent *Lawyer* and the *Lawyer* was made aware of all relevant circumstances known to the *auditor*, then the *auditor* may rely on such advice, provided the *auditor* has complied with auditing standards on using the work of an expert.

21.6.3 Reporting to regulators

Overview

79. Making a *SAR* to the *FIU* does not relieve the *auditor* of its other statutory reporting duties. Examples of these responsibilities include:

- **audits of *customers* carrying on *financial services business*:** The *auditor* has a statutory duty to report matters of "material significance" to the *JFSC* which come to the *auditor's* attention in the course of its audit work;
- **audits of *customers* in the public sector:** A*uditors* of some *customers* which operate in the public sector may be required to report on the *customer's* **compliance** with regulatory requirements around financial transactions. Activity connected with *money laundering* may constitute a breach of those requirements;
- **audits of other types of *customer*:** A*uditors* of some other types of *customers* are also required to report matters of "material significance" to regulators (for example, charities and occupational pension schemes).

21.6.4 Balancing professional work and post-reporting requirements

Overview

80. Continuation of audit work following the submission of an external *SAR* may require discussion of matters relating to the suspicions that were formed with the *customer's* board/senior management. Care must be taken to select appropriate and non-complicit members of the board/senior management for such discussions, keeping in mind the need to avoid tipping-off. It is important to confine enquiries to those required in the ordinary course of business and not attempt to further investigate a matter reported upon, unless this is within the scope of the professional work commissioned.

81. In more complex circumstances, consultation with the *FIU* may be necessary before enquiries are continued. It should be noted that neither the *FIU* nor other law enforcement agencies may give consent to tipping-off.

82. *Supervised persons* carrying on audit business may wish to engage their *MLRO/Deputy MLRO* or another suitable specialist (for example a *Lawyer*) if there are tipping-off concerns. In particular, it is important that before any document referring to the subject matter of a *SAR* is released to a third party, the *MLRO* (or *Deputy MLRO*) is consulted along with, where necessary, law enforcement. Some typical examples of documents released to third parties include but are not limited to:

- public audit or other attest reports;
- public record reports to regulators;
- confidential reports to regulators;
- statements on the resignation of a *supervised person* as *auditor*;
- professional clearance/etiquette letters; or
- communications to *customers* of a *supervised person's* intention to resign.

83. There is no legal mechanism for obtaining consent from the *FIU* regarding the contents of statements or other documents relating to an auditor's resignation. However, in complex cases, *supervised persons* carrying on audit business may still wish to discuss the matter with the *FIU* to understand their perspective and document such discussion.

84. *MLRO*s may, on occasion need advice to assist them in formulating their instructions to the *supervised person*. Legal advice may be sought from a suitably skilled and knowledgeable professional legal adviser, and recourse may also be had to helplines and support services provided by professional bodies. Discussion with the *FIU* may well be valuable, but *MLRO*s should bear in mind that the *FIU* and law enforcement are not able to advise, nor are they entitled to dictate, how professional relationships should be conducted.

21.6.5 Auditor's report on financial statements

Overview

85. Where it is suspected that *money laundering,* the *financing of terrorism,* or the *financing of proliferation* has occurred, the auditor will need to apply the concept of materiality when considering whether the auditor's report on the *customer's* financial statements needs to be qualified or modified, taking into account whether:

- the crime itself has a material effect on the financial statements;
- the consequences of the crime have a material effect on the financial statements; or
- the outcome of any subsequent investigation by the investigating agencies may have a material effect on the financial statements.

86. If it is known that *money laundering* or the *financing of terrorism* has occurred and members of the *customer's* board or senior management were knowingly involved, the auditor will need to consider whether their report will include a qualified opinion on the financial statements disclosing the same. Any such disclosure in the auditor's report will be subject to the tipping off requirements set out at section 9.5 of *this Handbook*. It might be necessary for the auditor, through the *MLRO* (or *Deputy MLRO*), to discuss with the relevant law enforcement agency whether disclosure in their report on the financial statements could constitute a tipping-off offence. If so, the auditor, through the *MLRO* (or *Deputy MLRO*), will need to seek guidance on an acceptable form of words with the *FIU*.

87. As noted at section 9.4 of *this Handbook*, the *FIU* is not able to advise or instruct in respect of a *supervised person's* professional conduct. Auditors must therefore bear this in mind when discussing a potential form of words with the *FIU* which can then be used in communicating with the *customer*. In circumstances like these, the auditor may also wish to consider seeking legal advice to reduce the risk of committing a tipping off offence.

88. A delay in issuing the audit report pending the outcome of an investigation may not be practicable for the auditor and could itself create a risk of tipping off.

89. If it is concluded that a qualified audit report must be issued, the *supervised person* may need to seek legal advice before issuing the report. In exceptional circumstances, it may be necessary to make an application to the court in respect of the content of the qualified audit report.

21.6.6 Resignation as auditor

90. If an auditor, having filed a *SAR*, wishes to terminate a *business relationship,* and is concerned that in doing so it may prejudice an investigation, it should seek guidance from the *FIU*. This will help reduce the risk of tipping-off. However, the *FIU* cannot instruct a *supervised person* to continue a *business relationship* that it wishes to terminate.

91. An auditor may wish to resign if it is believed that the *customer* or an employee of the *customer* is engaged in *money laundering*, the *financing of terrorism*, or the *financing of proliferation,* or any other illegal act, particularly where a normal relationship of trust can no longer be maintained. Where the auditor intends to resign, there may be a conflict between the requirements to bring certain matters to the attention of the *customer's* members or creditors and the risk of tipping-off. In such circumstances the auditor should seek guidance from the *FIU* and the appropriate investigating agency to discuss an appropriate course of action and an acceptable form of words. If necessary, legal advice or the direction of the court may need to be sought.

92. The risk of tipping-off may also cause a conflict with the need to communicate with the prospective successor auditor in accordance with ethical requirements relating to changes in professional appointments. Whilst the existing *auditor* might feel obliged to advise the incoming auditor of their suspicions of *money laundering,* the *financing of terrorism*, or any other illegal act, to do so would run the risk of tipping-off. Expressing suspicions orally rather than in writing **does not** constitute a mitigation of the tipping-off risk. In circumstances where it is considered necessary to communicate the underlying circumstances which gave rise to the *SAR*, guidance should be sought from the *MLRO* (or *Deputy MLRO*) who may then need to seek an opinion from the *FIU*.

PART IV: GLOSSARY

22 GLOSSARY

In addition to this Glossary, *Guidelines* are published on the *JFSC* website in relation to the interpretation of any provision in Schedule 2, including any expression used in Schedule 2 in accordance with Article 36(2) of the *Proceeds of Crime Law*.

Term	Definition
accountancy services	Has the meaning given in paragraph 22 of Part 3 of Schedule 2 to the *Proceeds of Crime Law* and as further defined in Section 3.25.1 of the *Guidelines*.
Accountant(s)	Persons carrying on business described at paragraph 23 of Part 3 of Schedule 2 to *Proceeds of Crime Law.*
AML	*Anti-money laundering.*
AML/CFT/CPF	*Anti-money laundering/countering the financing of terrorism/countering proliferation financing.*
AML/CFT/CPF programme	A programme against *money laundering, terrorist financing, and proliferation financing* which includes *policies and procedures* by which every member of the group who carries on a *financial services business* (or equivalent) shares information that is appropriate for the purpose of preventing and *detecting money laundering, terrorist financing,* and *proliferation financing.*
AML/CFT/CPF Codes of Practice	*Codes of Practice* for *supervised persons*, issued under Article 22 of the *Supervisory Bodies Law*. This includes Codes in Sections 1 to 10 that relate to all *supervised persons* (except *NPOs*) and Codes that relate to particular activities in the sector-specific Sections 11-16 and 18.
AML/CFT/CPF Handbook	*Handbook* for the prevention and detection of *money laundering*, the countering of *terrorist financing*, and the countering of *proliferation financing.* May also be referred to as "*the Handbook*" or "*this Handbook*".
AML/CFT/CPF obligations	*AML/CFT/CPF obligations* under *Anti-Money Laundering and Counter-Terrorism Legislation* and the *AML/CFT/CPF Handbook.*
Anti-Money Laundering and Counter-Terrorism Legislation	Has the meaning given in Article 3(1) of the *Supervisory Bodies Law*.
AMLSP	*Anti-money laundering services provider* is the service provider appointed by an eligible *supervised persons* in accordance with Article 9A of the *Money Laundering Order.*
AMLSP Direct Customer	Means a *customer* of an *AMLSP* that is itself a Schedule 2 *Business* in receipt of *AMLSP services* from the *AMLSP.*

Term	**Definition**
AMLSP Direct Customer MLCO	Means an *AMLSP Direct Customer*'s *MLCO,* being an individual appointed by the *AMLSP* to fulfil the *MLCO* function on behalf of its *AMLSP Direct Customer.*
AMLSP Direct Customer MLRO	Means an *AMLSP Direct Customer*'s *MLRO,* being an individual appointed by the *AMLSP* to fulfil the *MLRO* function on behalf of its *AMLSP Direct Customer.*
AMLSP Indirect Customer	Means a *customer* of the *AMLSP Direct Customer* and includes third parties for whom the *AMLSP Indirect Customer* acts.
AMLSP services	Means services provided by a *AMLSP* to an *AMLSP Direct Customer* that enable the *AMLSP Direct Customer* to fulfil its *AML/CFT/CPF obligations*
ATM	An automatic teller machine, a machine that allows bank transactions without bank representative interaction.
audit services	Has the meaning given in paragraph 22(3) of Part 3 of Schedule 2 to the *Proceeds of Crime Law.*
Banking Services	With regard to Correspondent Banking, it refers to any of the following: • providing a current or other liability account; • cash management; • international funds transfers; • cheque clearing; • providing *customer*s of the respondent with direct access to accounts with the correspondent (and vice versa); and • providing foreign exchange services
Basel Committee	Basel Committee on Banking Supervision.
BB(J) Law	Banking Business (Jersey) Law 1991.
Beneficial owners and/or controllers	Has the meaning set out in Article 2 of the *Money Laundering Order.* May also be referred to as "*beneficial owner*", "*owner*" or "*controller*" separately throughout the text.
BRA	*Business Risk Assessment*.
business relationship	Has the meaning set out in Article 1 of the *Money Laundering Order*. Certain professions may refer to a *business relationship* as a "matter".
CDD	*Customer* due diligence.
CD regulated TCSP	*TCSP* regulated by the *JFSC*, the Guernsey Financial Services Commission or the Isle of Man Financial Services Authority.
CFT	Countering the *financing of terrorism*.
CIF(J) Law	Collective Investment Funds (Jersey) Law 1988.
Collective investment scheme	Means any of the funds specified in Article 13(10) of the *Money Laundering Order.*
Commission Law	Financial Services Commission (Jersey) Law 1998.
Companies Law	Companies (Jersey) Law 1991.
Compliance Officer	Has the meaning given in Article 1 of the *Supervisory Bodies Law*.
Correspondent	In connection to *Correspondent Banking,* a person providing *Correspondent Banking* services

Term	Definition
Correspondent Banking	The provision of Banking Services by a Financial Institution or VASP (the correspondent) to a Financial Institution or VASP that itself provides Banking Services to its *customer*s (the respondent).
CPF	Countering *proliferation financing.*
CRA	*Customer* risk assessment.
customer(s)	A person with whom a *business relationship* has formed or *one-off transaction* carried out. References to *customer* also include, where appropriate, a prospective *customer* (an applicant for business) with whom a *business relationship* is to be established, or *one-off transaction* carried out. A *customer* may be a natural person (or group of individuals) or a legal person. May also be referred to by Industry as a 'client'. Supplemented by the *Guidelines* issued by the *JFSC*.
Customer due diligence measures	Has the meaning given in Article 3 of the *Money Laundering Order. May be referred to as CDD.*
customer(s) of obliged person	Has the meaning given in Article 16 of the *Money Laundering Order (for* section 5 of *this Handbook*).
Deposit-taking business	Has the meaning given in paragraph 2(2) of Part 2 of Schedule 2 to *the Proceeds of Crime Law*.
Deputy MLRO	A person designated by the *supervised person* to whom *SARs* may be made.
designated person	Has the meaning given in Article 9 of the *Sanctions and Asset-Freezing Law*.
Designated relationship (s)	A relationship established by a *customer* on behalf of one third party, including a relationship involving sub-accounts for each third party.
Designation	With regard to Article 3(4), part 4 or Part 5 of the *Sanctions and Asset-Freezing (Jersey) Law 2019*
Digital ID	Electronic Identification.
Directions Law	[*Money Laundering* and Weapons Development (Directions) (Jersey) Law 2012.]
DNFBP	*Designated Non-Financial Businesses and Professions* as defined in the *FATF* glossary. Refers to activities/operations specified in Part 3 of Schedule 2 to the *Proceeds of Crime Law*.
DPRK	Democratic People's Republic of Korea.
DBS	Disclosure and Barring Service is the UK Government's agency for criminal record disclosures
DBS check or equivalent	A certificate containing details of spent and unspent convictions provided by the DBS or an equivalent body in a foreign jurisdiction
Electronic Communications Law	[Electronic Communications (Jersey) Law 2000.]
EEA	European Economic Area.

Term	**Definition**
Employee or employee	Includes officers of a *supervised person* and is not limited to individuals working under a contract of employment. Includes temporary and contract *employees*, and the *employee* of any external party fulfilling a function in relation to a *supervised person* under an outsourcing agreement.
Enhanced *customer* due diligence (measures) or enhanced CDD measures	Has the meaning given in Article 1 of the *Money Laundering Order*. May also be referred to EDD or ECDD.
enhanced risk state	Has the meaning given in Article 15(1)(c) of the *Money Laundering Order*. Refer to **Appendix D1** of the *AML/CFT/CPF Handbook* for the current list of *enhanced risk states*.
equivalent business	Has the meaning given in Article 5 of the *Money Laundering Order.*
EU	The European Union.
EU Directive	EU Electronic Money Directive 2009.
EU Regulation	Regulation (EU) 2015/847 of 20 May 2015 on information accompanying transfers of funds.
Exemption Order	Proceeds of Crime (Low Risk Financial Services Business) (Jersey) Order 2024
express trust(s)	As defined in the *FATF* glossary and refers to activities/operations listed under Part 5 of Schedule 2 to the *Proceeds of Crime Law*.
external accountancy services	Has the meaning given in paragraph 22(4) of Part 3 of Schedule 2 to the *Proceeds of Crime Law*.
Facilitator(s)	An active supporter of a terrorist, terrorist cell or terrorist organisation, e.g., a *terrorist financier*, a regulated and registered professional or a recruiter.
FATF	The Financial Action Task Force.
FATF Recommendations	The *FATF* Recommendations adopted on 16th February 2012 and as amended from time to time.
Financial crime	*Financial crime* means: a. *Money laundering* b. The *financing of terrorism* c. Offences related to *money laundering* or the *financing of terrorism*
financial group(s)	A collection of persons who are members of the same group, each person fulfilling the conditions set out in Article 1(5) of the *Money Laundering Order*.
Financial Institution(s)	As defined in the *FATF* glossary. Refers to activities/operations specified in Part 2 of Schedule 2 to the *Proceeds of Crime Law*.
financial services business(es)	Has the meaning in Article 36 of the *Proceeds of Crime Law.*
financing of proliferation or *proliferation financing*	For the purposes of *this Handbook*, this term means:

Term	Definition
	Conduct which creates the risk of non-implementation, breaching, circumvention, or evasion of the Targeted financial sanctions related to proliferation of weapons of mass destruction and its financing, effective in Jersey. Persons involved in the *financing of proliferation* are sometimes described as *proliferators* or *proliferation financiers*.
financing of terrorism or terrorist financing	• Conduct which is an offence under any provision of Articles 15, 16 and 16A of the Terrorism (Jersey) Law 2002 [the Terrorism Law]; • Conduct outside Jersey which, if occurring in Jersey, would be an offence under Articles 15, 16 and 16A of the Terrorism Law; • Conduct which is an offence under any provision of Article 21 of the Terrorism Law; and • Conduct which is an offence under any provision of Parts 3, 4 and 6 of the Sanctions and Asset-Freezing Law. • Persons involved in the *financing of terrorism* are sometimes described as terrorist financiers.
FIU	The Financial Intelligence Unit for Jersey as designated by the regulations made under 41B of the Proceeds of Crime (Jersey) Law 1999
Foundations Law	Foundations (Jersey) Law 2009.
Foreign financial institution	Means a person who carries on financial business falling within Part 2 (financial institutions) of Schedule 2 to the Law outside Jersey and is not a Jersey financial institution
Foreign VASP	A person that is not incorporated or constituted under the law of Jersey and carries on such financial services business in any part of the world
FSIU	Financial Sanctions Implementation Unit, forming part of Jersey's Ministry of External Relations.
FS(J) Law	Financial Services (Jersey) Law 1998.
FSRB	*FATF* Style Regional Body.
Governing body	Means the body that is considered to be exercising ultimate control of a legal person or arrangement. Generally, this will be board of directors of: • a company, *PCC*, *ICC* or the incorporated cells of an *ICC*; • the trustee of a trust; • the general partner of a limited partnership, a separate limited partnership or incorporated limited partnership or the partners of a limited liability partnership; • the manager or if no manager, the managing members of a limited liability company; • the council of a foundation.
Guidance notes	Present ways of complying with the *statutory requirements* and *AML/CFT/CPF Codes of Practice* and must always be read in conjunction with these.

Term	Definition
Guidelines	Means *Guidelines* issued by the *JFSC* on the interpretation of any provision in Schedule 2, including any expression used in Schedule 2 in accordance with Article 36(2) of the *Proceeds of Crime Law*.
Hawala	Hawala refers to a traditional system of transferring money without money movement. It is done with the help of a brokering third party, and it is predominantly used in the Middle East, Africa, and South Asia. These payment systems may also be referred to as Hundi or Havala.
high value dealer	Has the meaning given in paragraph 20 of Part 3 of Schedule 2 to the *Proceeds of Crime Law.*
higher risk country or territory	A country or territory which a *supervised person* has concluded presents a higher risk of *money laundering*, the *financing of terrorism*, and the *financing of proliferation*, using reliable and independent third-party sources.
IAIS	International Association of Insurance Supervisors.
IB(J) Law	Insurance Business (Jersey) Law 1996.
ICC	Incorporated cell company.
identification measures	Those measures described in Article 3(2) of the *Money Laundering Order*.
IFSWF	International Forum of Sovereign Wealth Funds.
IMF	International Monetary Fund.
Information Order	Proceeds of Crime (Provision of Information by Trustees) (Jersey) Order 2021.
insolvency practitioner	Those in the business of undertaking *insolvency services*.
insolvency services	Has the meaning given in paragraph 22(4) of Part 3 of Schedule 2 to the *Proceeds of Crime Law*.
IOSCO	International Organization of Securities Commissions.
Jersey competent authority	Any person other than the *FIU* that exercises a public function concerned with the prevention, investigation, detection or prosecution of *financial crime*.
JFSC	Jersey Financial Services Commission (abbreviated in relevant Jersey legislation as the "*Commission*").
Jersey financial institution	a) A person who carries on financial services business falling within Part 2 (financial institutions) of Schedule 2 *to the Law* in or from within Jersey; or b) A person that is incorporated or constituted under the law of Jersey and carries on such financial services business in any part of the world.
Jersey VASP	a) A person who carries on financial business falling with Part 4 (virtual asset service provider) of Schedule 2 to the *Proceeds of Crime Law* or b) A person that is incorporated or constituted under the law of Jersey and carries on such financial services business in any part of the world.
Lawyer	Persons carrying on the business described at paragraph 21 of Part 3

Term	Definition
	of Schedule 2 to the *Proceeds of Crime Law*.
Licence	A generic term to cover: › A registration granted under the *BB(J) Law* › A permit granted pursuant to the *CIF(J) Law* › A certificate issued pursuant to the *CIF(J) Law* › A registration granted under the *FS(J) Law* › A permit granted pursuant to the *IB(J) Law*.
limited liability company	Has the meaning given in Article 1(1) of the *Money Laundering Order.*
LPP	Legal professional privilege. This term covers both advice privilege and litigation privilege (see section 15.7.1 *of this Handbook*).
(the) Minister	Unless otherwise specified, means the Minister for External Relations and Financial Services.
MLCO	*Money Laundering Compliance Officer*, as described in Article 7 of the *Money Laundering Order*.
MLRO	*Money Laundering* Reporting Officer, as described in Article 8 of the *Money Laundering Order*. Also refer to *Deputy MLRO* above.
money laundering	For the purposes of *this Handbook*, means: › Conduct which is an offence under any provision of Articles 30 and 31 of the *Proceeds of Crime Law*; › Conduct which is an offence under any provision of Articles 34A and 34D of the *Proceeds of Crime Law*; and › Conduct which is an offence under any provision of the Sanctions and Asset-Freezing (Jersey) Law 2019 or any provision of an Order under Article 3 of that Law; and › Conduct which falls within the definition of *financing of terrorism* set out in *this Handbook*. Persons involved in *money laundering* are sometimes described as *money launderers*.
Money Laundering Order	*Money Laundering* (Jersey) Order 2008.
MVTS	Money or Value Transfer Services. means a person who provides a money or value transfer service within the meaning given in paragraph 5 in Part 2 of Schedule 2 to the *Proceeds of Crime Law.*
non-professional trustee	Means a natural person acting, as trustee of an *express trust* as referred to in paragraph 25 of Part 5 of Schedule 2 to the *Proceeds of Crime Law*, whose activity is not conducted as a business.
NPO	Non-profit organisations defined under Article 1 of the *NPO Law*. The definitions extend to both *Regulated NPOs* and *Registered NPOs.* The sector, including all *NPOs* may also be referred to as the non-profit sector.

Term	Definition
NPPS	New Payment Products and Services.
obliged person(s)	Has the meaning given in Article 1 the *Money Laundering Order*.
one-off transaction	Has the meaning given in in Article 4 of the *Money Laundering Order*.
Overseas Competent Authority	An external authority that has equivalent function to those of Jersey.
Payment Service Provider	Means a person, being a person registered under the *Banking Business (Jersey) Law 1991* or who is a virtual asset service provider or a money or value transfer service provider, when- (a) The person is carrying out payment services in or from within Jersey; or (b) Being a legal person established under Jersey law, the person is carrying out payment services in any part of the world other than in or from within Jersey.
PCC	A protected cell company.
PEP	Politically Exposed Person – an individual who is any of the following (within the meaning of Article 15A of the *Money Laundering Order*: (a) A domestic politically exposed person; (b) A foreign politically exposed person; or (c) A prominent person.
policies and procedures	The way in which a business' *systems and controls* are implemented into the day-to-day operation of the business.
pooled relationship	A relationship established by a *customer* on behalf of more than one third party.
Prescribed NPO	Has the meaning given in Article 1 of the *Prescribed NPO Order*. The sub-set of *NPOs* which present a higher risk of being abused for *terrorist financing* purposes.
Prescribed NPO Order	Prescribed Non-profit Organisations (Jersey) Order 2022.
Proceeds of Crime Law	Proceeds of Crime (Jersey) Law 1999.
proliferation financing	Refer to the definition of *financing of proliferation*.
prominent public function	In relation to an international organisation, means a member of the senior management, including a director, deputy director, board member or other equivalent function.
Proscribed terrorist organisation	Individuals or organisations that are placed on national and international lists of actors known to be engaged in terrorist activities. Jersey's *Proscribed terrorist organisation* list may be accessed in Schedule 1 of *Terrorism Law.* Part 2 of the *Terrorism Law* sets out that the UK's proscribed list automatically forms part of the Jersey proscribed list, hence both lists must be considered.
public authority	A person holding a public office in Jersey.
real estate agent	Has the meaning given in paragraph 19 of Part 3 of Schedule 2 to the *Proceeds of Crime Law.*

Term	Definition
regulated business	Has the meaning provided given in Article 1 of the *Supervisory Bodies Law*.
regulated market	Has the meaning given in Article 2(5) of the *Money Laundering Order.* To access the list of *EU-regulated market*s, follow this link and select '*Regulated Market*' from the 'Entity Type' drop-down list.
regulated person	Has the meaning given in Article 1 of the *Supervisory Bodies Law*.
Regulatory Laws	A collective name of the following laws: › The *BB(J) Law*; › The *CIF(J) Law*; › The *FS(J) Law*; › The *IB(J) Law*; and › The Alternative Investment Funds (Jersey) Regulations 2012.
reliance identification measures	Has the meaning given in Article 16(1) of the *Money Laundering Order*.
relevant connection	Has the meaning given in Article 15(2)(b) of the *Money Laundering Order*.
relevant employee	An employee whose duties relate to the provision of a *financial services business*.
relevant financial institution	Has the meaning given in Article 1 of the *Sanctions and Asset-Freezing Law.*
relevant *customer*	Has the meaning given in Article 17 of the *Money Laundering Order.*
relevant person	Means, for the purposes of *this Handbook*, a person carrying on a *financial services business* (as described in Schedule 2 of the *Proceeds of Crime Law*), and which is carrying on that business in or from within Jersey, or, if a Jersey legal person, carrying on that business in any part of the world. Where specific articles of the *Money Laundering Order* proscribe that the term *relevant person* includes a person who **was formerly** a *relevant person*, any references to *relevant person* in *this Handbook* that relate to or are derived from those particular articles should also have the same meaning. From 1 October 2023 to the end of 30 September 2024, this definition **does not** capture a *specified director* who from the commencement of the *Proceeds of Crime Law* 2022 acted as a director of a company and in so acting conducted a business that became a *financial service*s business in terms of paragraph 23(2) of Schedule 2 of the *Proceeds of Crime law.*
Respondent	In connection to *Correspondent Banking*, the person provided with *Correspondent Banking* services
Risk Questionnaire	*JFSC*'s annual (or ad hoc) Supervisory Risk Data Collection Questionnaires, as amended from time-to-time.

Term	Definition
sanctioned country or territory	Means, at any time, a country or territory which is itself, or whose government (or equivalent) is, the subject of any sanctions broadly prohibiting dealings with such government (or equivalent), country or territory, including trade sanctions, arms embargoes and other trade restrictions in force in Jersey (refer to Sources 6 and 12 of **Appendix D2** of *this Handbook* for a current list of sanctioned countries and territories).
sanctioned person	Means a person or entity listed on the sanctions designations lists under the Jersey sanctions regime.
Sanctions and Asset-Freezing Law	Sanctions and Asset-Freezing (Jersey) Law 2019.
SAR	Suspicious Activity Report.
Senior executives of state-owned corporations	In relation to identifying PEPs, *senior executives of state-owned corporations* are those individuals with executive decision-making authority. This would not normally include non-executive directors, where they do not have such authority.
sensitive activities	Refers to activities that have been established, as a matter of policy, by the *JFSC* as *sensitive activities*, and which are listed in the *JFSC's* Sound Business Policy.
similar identification measures	Has the meaning given in Article 16A(1) of the *Money Laundering Order.*
similar relationships	In connection to *Correspondent Banking,* those where financial services (but not *Banking Services*) are provided to an overseas *Financial Institution* or *VASP*
sole trader	Has the meaning given in Article 1 of the *Money Laundering Order*.
source of funds	The activity that generates the funds for a *customer* (e.g., salary, trading revenues, or payments out of a trust). *Source of funds* relates directly to the economic origin of funds to be used in a *business relationship* or *one-off transaction*.
source of wealth	The activities that have generated the total net worth of a *customer* (e.g., ownership of a business, inheritance, or investments). *Source of wealth* is the origin of the accrued body of wealth of an individual.
SPV	Special Purpose Vehicle. An entity established for a specific purpose, e.g., to act as a *Governing body* of a specific fund.
Specified director	A person who, on or after the commencement of the *Proceeds of Crime Law 2022*: (a) acted as a director of a company; and (b) in so acting conducted a business that became *a financial services business* because of paragraph 23(2) of Schedule 2 to the Proceeds of Crime (Jersey) Law 1999. (N.B. this will be repealed on 1 October 2024).
spent convictions	As defined in Article 2 of the Rehabilitation of Offenders (Jersey) Law 2001

Term	Definition
statutory requirements	Describe the statutory provisions that must be complied with by a *supervised person* (natural or legal) when carrying on a Schedule 2 *business*, in particular requirements set out in the *Money Laundering Order.*
supervised business	Has the meaning given in Article 1 of the *Supervisory Bodies Law*.
supervised person	Defined in Article 1 of the *Supervisory Bodies Law* and covers all those persons that are required to comply with the *Money Laundering Order* (referred to in the *Money Laundering Order* as "*relevant persons*"). References in *this Handbook* where legislation is quoted, summarised, or paraphrased will be to *relevant persons* to align with the *Money Laundering Order.* ***Note: Directors registered as TCSPs but who are not TCBs are subject to reduced requirements as per the Exemption Order.***
Supervisory Bodies Law	Proceeds of Crime (Supervisory Bodies) (Jersey) Law 2008.
Sympathiser(s)	An individual who is *not actively* engaged in terrorist acts but that supports individual terrorists, terrorist cells or terrorist organisations indirectly.
systems and controls	A *supervised person's* general framework to combat *money laundering,* the *financing of terrorism,* and the *financing of proliferation*.
Targeted Financial Sanctions Measures	*Targeted Financial Sanctions Measures* include any measures made under: › The *Sanctions and Asset-Freezing Law* › Any Regulations or Orders made under the enactment falling within the above law (e.g. the Sanctions and Asset-Freezing (Implementation of External Sanctions) (Jersey) Order 2021).
tax adviser	Persons providing, by way of business, the service set out at paragraph 22(3)(b) of Part 3 of Schedule 2 to the *Proceeds of Crime Law*.
Terrorism and related terms	"*Terrorism*", "*act of terrorism"* and "*terrorist entity*" are defined in the *Terrorism Law*. "Terrorist activity" is defined in Article 18 of the *Sanctions and Asset-Freezing Law.* For the purposes of *this Handbook*, Targeted financial sanctions related to terrorism and *terrorist financing* are those described on the *JFSC's* website.
Terrorism Law	Terrorism (Jersey) Law 2002.
terrorist financing	Refer to the definition of *financing of terrorism.*
TF Recruitment	Active and passive processes through which *terrorists, terrorist cells* and *terrorist organisations* seek to enlist operational personnel, facilitated by a recruiter.

Term	Definition
TFS	The term "targeted financial sanctions" means both asset freezing and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of *designated persons* and entities.
Third party identification requirements	Has the meaning given at Article 17 of the *Money Laundering Order*.
Tipping Off Regulations	Proceeds of Crime and Terrorism (Tipping Off – Exceptions) (Jersey) Regulations 2014.
TCSP or trust and company service provider	As defined in the *FATF* glossary and refers to activities/operations specified in paragraph 23 of Part 3 of Schedule 2 to *the Proceeds of Crime Law*.
Trust Company Business	Subject to any Order under Article 4 of the *FS(J) Law*, has the meaning given at Article 2(3) of the *FS(J) Law*. Persons carrying on *Trust Company Business* may also be referred to as "*Trust and company service providers*" or "*TCSPs*".
Trust Law	Trust (Jersey) Law 1984.
UK	The United Kingdom.
UN	The United Nations.
unit	Has the meaning given in Article 1(1) of the *CIF(J) Law*.
UNSC	The United Nations Security Council.
VA	Virtual Asset. A digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes.
VASP	Virtual Asset Service Provider. Has the meaning given in paragraph 24 of Part 4 of Schedule 2 to the *Proceeds of Crime Law*. To assist with the interpretation of *VASP* activities and operations, refer to the *Guidelines*.
VAT	Value Added Tax.
Virtual currency exchange business	Means the business of conducting one or more of the activities or operations to, for or on behalf of another natural or legal person or arrangement set out in paragraph 24(2)(a), (b) and (c) of Part 4 of Schedule 2 to the *Proceeds of Crime Law.*
Wire Transfer Regulations	EU Legislation (Information Accompanying Transfers of Funds) (Jersey) Regulations 2017.