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 *customer*s".

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 4.3 of *this Handbook* with a *customer* who is an individual (or group of individuals), section 4.4 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 of the Money Laundering Order. 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	✓	✓ **OR**
Date of birth	✓	✓

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 4.3.3 of *this Handbook*);
- external data sources (see section 4.3.4 of *this Handbook*); and/or
- *Digital ID* (see section 4.4.5 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 4.3.4 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 4.3.4 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 4.3.4 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 4.4.5 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 64 below and **adequate information** as set out in paragraph 66 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 67 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 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 60 and 61 above. This would create an electronically certified document.

63. 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.

64. 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.

65. 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.

66. 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

67. 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 64 above and **adequate information** as set out in paragraph 66 above;
- certification which includes an image or photograph affixed to a document which is not an electronic signature as described within paragraphs 60 and 61 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.

68. The *JFSC* considers that certification by a suitable certifier, in line with the guidance set out at section 4.3.3 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

69. 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.

70. 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

71. 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.

72. 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

73. 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*.

74. The FATF has issued Guidance on Digital Identity, March 2020 which *supervised person*s 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.

75. 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.

76. 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?

77. 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.

78. 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.

79. **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

80. 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)

81. *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.*

82. *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

83. Using a *Digital ID* application is one way of obtaining evidence of identity. Section 4.3.2 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.

84. As an alternative to using documentary evidence, section 4.3.2 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.

85. 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)

86. *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.*

87. *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

88. 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.

89. 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.

90. 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.

91. 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.

92. 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.

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

4.3.5.2 Risks of using Digital *ID*

Overview

94. 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

95. 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.

96. 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.

97. 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.

98. 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.

99. 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

100. 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.

101. 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

102. 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.

103. 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.

104. 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

105. 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.*

106. 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

107. 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.

108. 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

109. 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.

110. 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.).

111. 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

112. On occasions, an individual may be unable to provide evidence of identity using the sources set out at section 4.3.2 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

113. 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.

114. 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.

115. 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.

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

4.3.7 Residential address: Overseas residents

Overview

117. 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 4.3.2 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.

118. 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

119. 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.

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 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.

121. 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

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

123. 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 4.5 of *this Handbook.*

124. 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 schemes* – known as unit trusts.

125. 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).

126. 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.

127. 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*).

128. 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*.

129. 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*.

130. 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*.

131. 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.

132. 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.

133. 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.

134. 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

135. 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).

136. 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.

137. This information may be provided by the trustee.

138. 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.

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 who has been identified as presenting higher risk. 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 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.

141. 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.

142. 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.

143. 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 o*f this Handbook* for a graphical explanation of the process described in the paragraph above.

144. 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

145. 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

146. 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).

147. 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.

148. 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.

149. 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.

150. In any case where a partner (including a general 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)(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.

151. 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.

152. 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

153. 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).

154. 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.

155. 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.

156. 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.

157. 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

158. 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.

159. 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*.

160. 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.*

161. 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.*

162. 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*.

163. 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

164. 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".

165. 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.

166. 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.

167. 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."

168. 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*).

169. 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.

170. 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

171. 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.

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

173. 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*.

174. 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.

175. 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.

176. 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.

177. 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.*

178. 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.

179. 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.

180. 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.

181. 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.

182. 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.

183. 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*.

184. 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.

185. 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

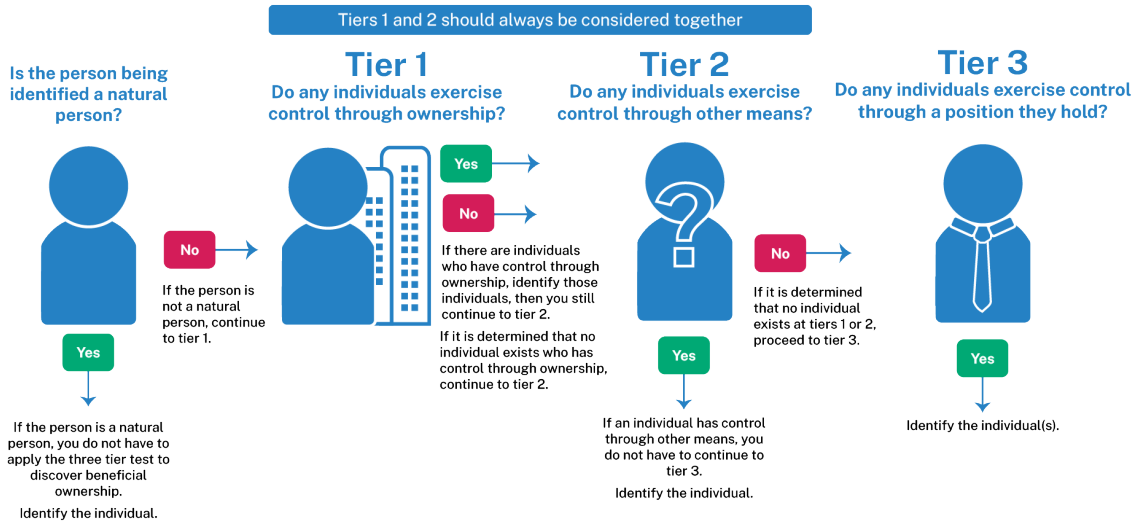
Guidance notes

186. 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.

187. 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.

188. The above information may be provided by the company.

189. 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).

190. 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.

191. 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

192. 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).

193. 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.

194. 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 *customer*s):

- 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.

195. 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.

196. 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

197. 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.

198. 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.

199. The above information may be provided by the foundation.

200. 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.

201. 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*.

202. 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

203. 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).

204. 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.

205. 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.

206. 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).

207. 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

208. 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).

209. 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.

210. 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).

211. 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).

212. This information may be provided by the partnership.

213. 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.

214. 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.

215. 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

216. 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).

217. 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.

218. 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 *customer*s):

- 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.

219. 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.

220. 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

221. 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.

222. 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*.

223. 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*.

224. 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.*

225. 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*.

226. 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)

227. *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

228. 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.

229. 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.

230. Control through other means is ultimate effective control which is more than minor influence.

231. 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.

232. 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*.

233. 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.

234. Examples of how good practice may be demonstrated and documented in identifying controls by other means:

- Ask the customer to identify all controllers (including controllers by other means).
- Confirm any persons who 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)

235. *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.*

236. *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.*

237. *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

238. 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.

239. 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.

240. 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)

241. *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)).*

242. *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

243. 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.

244. 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).

245. 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.

246. 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.

247. 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.

248. 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.

249. 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

250. *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.*

251. *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.*

252. *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.*

253. *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.*

254. *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.*

255. *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>

256. *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.*

257. *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>

258. *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.*

259. *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).*

260. *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.*

261. *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.*

All cases

262. *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

263. 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*).

264. *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.

265. 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

266. 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.

267. 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.

268. 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).

269. 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

270. 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.

271. 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.

272. 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.

273. 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

274. *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.*

275. For the purposes of the *Money Laundering Order,* the meaning of existing customer depends on 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.

276. 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.

277. 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.

278. Higher risk existing/legacy *customer*s will be subject to the same programme of enhanced monitoring as any new high-risk *customer*.

279. 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.*

280. 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

281. 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).

282. 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).

283. 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*.

284. 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)

285. *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.*

286. *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.*

287. *Article 14(5) of the Money Laundering Order requires a relevant person to terminate a business relationship where it cannot apply ongoing identification measures.*

288. *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.*

289. *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

290. 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.

291. 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.

292. 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.

293. 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*.

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