

4 IDENTIFICATION MEASURES – FINDING OUT IDENTITY AND OBTAINING EVIDENCE

4.1 Overview of section

1. The purpose of this section of the *AML/CFT Handbook* is to explain 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* in order to assess the risk that any *business relationship* or *one-off transaction* will involve *money laundering* or the *financing of terrorism*, 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 in order to address the case of a *customer* that is assessed as presenting a higher risk of *money laundering* or the *financing of terrorism*, which is covered in Section 7.
3. Guidance is also given on the timing of obtaining evidence of identity and what to do where it is not possible to complete *identification measures*. This guidance covers all elements of *identification measures*, including, where appropriate, the collection of information under Article 3(5) of the *Money Laundering Order*.
4. The requirement to find out identity and obtain evidence (part of the *identification measures* referred to in Article 3 of the *Money Laundering Order*) applies:
 - › at the outset of a business relationship or one-off transaction
 - › where there is suspicion of money laundering or the financing of terrorism
 - › where there is some doubt as to the veracity or adequacy of documents, data or information that are already held (including the circumstances set out in Paragraph 5 below)
 - › in respect of “existing customers”.
5. As stated in Section 3.4 of this Handbook, the requirement to find out identity and obtain evidence will also apply when there are changes, for example a:
 - › 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 deals with a customer who is an individual (or group of individuals), Section 4.4 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 deals with a customer who is a legal person.
7. The term *customer* is defined in the Glossary above.



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, *E-ID* (see Section 4.3.5) and, in appropriate circumstances, written assurances from *obliged persons*.
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 Section 3. Among other things, identification measures must establish the persons who are concerned with a legal arrangement, and each beneficial owner and controller of a customer who is a legal person.*
12. *Under Article 3(2)(b) of the Money Laundering Order a relevant person must determine whether a customer is acting for a legal arrangement, and, if so, identify the legal arrangement.*
13. *Where a customer is acting for a legal arrangement, Article 3(2)(a) of the Money Laundering Order requires the customer, e.g. the trustee of a trust or general partner of a limited partnership, to be identified.*
14. *Article 3(2)(b)(iii) of the Money Laundering Order requires the identity of each person who falls within Article 3(7) 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) who is not an individual, Article 3(2)(b)(iii) requires each individual who is that person's beneficial owner 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) 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 or controller*
- › the *beneficial 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 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 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 of the following:

- › 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 and
- › government issued personal identification number or other government issued unique identifier.

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 of the following:

- › legal name, any former legal name(s), and any other name(s) used
- › principal residential address
- › date of birth.

4.3.2 Obtaining evidence of identity

Overview

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



- › original documents (see Section 4.3.2);
 - › certified copies of documents (see Section 4.3.3);
 - › external data sources (see Section 4.3.4); and/or
 - › *E-ID* (see Section 4.3.5).
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. For E-ID applications, the technology used may not sufficiently mitigate the inherent risks associated with it. Therefore, a supervised person will need to ensure that its CDD systems and controls incorporate measures specifically designed to do so – see Section 4.3.5.
 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. They 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 risk (see Section 3.4 of this Handbook for more detail).

AML/CFT Codes of Practice

28. 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 *JFCU* or the *JFSC*.



Guidance notes

29. 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 31):

- › legal name and name(s) currently used
- › principal residential address
- › date of birth
- › place of birth
- › nationality and
- › passport or national identity number.

30. 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 31):

- › legal name and other names used and
- › principal residential address (or, as an alternative, date of birth).

For the avoidance of doubt, this paragraph may be applied to *customers* who are resident outside of Jersey.

31. 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
<ul style="list-style-type: none">› 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:
<ul style="list-style-type: none">› correspondence from a central or local government department or agency (e.g. States and parish authorities)› a letter of introduction confirming residential address from:


Residential address:

- 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.

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. 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) or, in the case of a residential address, personal visit to that address.
34. 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 on-going correspondence with that customer at the changed address.
35. 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 FATF-Style Regional Bodies.



4.3.2.1 Electronic bank statements and utility bills

Overview

36. 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**).
37. 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)

38. *Article 3(2)(a) of the Money Laundering Order states that identification measures are for identifying the customer.*
39. *Article 3(4)(b) of the Money Laundering Order states that for the purposes of Article 3(2), 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

40. 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*.
41. 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.
42. 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.
43. 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 below) 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.



44. 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.
45. Consideration should be given to whether concerns regarding the integrity of the electronic statement warrant a SAR.

4.3.3 Suitable certification

Overview

46. 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 into 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) are applied through a trusted external party and where the *customer* (or other person) is physically present.
47. *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 is relevant.
48. **Nor** should the provisions in Section 4.4.5 and Section 4.5.7 for copy documentation to be provided by a **supervised Trust and Company Services Provider** be confused with **suitable certification**.

Guidance notes

49. 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.
50. 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](#))
 - › 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.
51. 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 other *FSRBs*.
52. 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.
53. 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

54. A *suitable certification* may take the following forms:
- › a hand-written certification which meets the criteria as described in paragraphs 55 and 56; or
 - › an electronic certification which is produced using software as described in paragraph 57.
55. 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 61 and **adequate information** as set out in Paragraph 63 so that they may be contacted in the event of a query.
56. On 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 64 to **validate** the credentials of the suitable certifier.
57. **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 in order for it to be acceptable.
- Article 9A of the Electronic Communications (Jersey) Law 2000 (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.



58. 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)).
59. In the case of the affixation of an electronic signature to certify a document, we would expect that the suitable certifier is in receipt of the relevant original documentation (as described in 4.3.2) 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 57 and 58. This would create an electronically-certified document.
60. It is not a requirement for a document which has been electronically certified to be received directly from the certifier.
61. 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.
62. 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.
63. 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.
64. 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* and the *financing of terrorism* 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

65. 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 61 and **adequate information** as set out in Paragraph 63;



- › certification which includes an image or photograph affixed to a document which is not an electronic signature as described within Paragraphs 57 and 58;
 - › 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.
66. The *JFSC* considers that certification by a *suitable certifier*, in line with the guidance set out at Section 4.3.3, 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

67. Independent data sources can provide a wide range of confirmatory material on the identity of a *customer* and can be accessible, for example, through publically 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.
68. 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

69. 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.
70. 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 information.

4.3.5 Use of electronic identification (E-ID)

Overview

71. 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 *E-ID*). this section will provide guidance and (where relevant) set out *AML/CFT 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 *E-ID* applications
 - › examples of risk mitigants to consider when assessing the potential use of a particular *E-ID* method or application and
 - › examples of practices or methods which are not considered to be *E-ID*.
72. The FATF has issued [guidance on Digital Identity, March 2020](#) which *supervised persons* may find useful in developing their own procedures and controls.
73. 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.
74. In order to adequately consider the risks associated with *E-ID*, the *supervised person's* Board/senior management should clearly identify, fully understand and document what the *E-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?
75. Where it is identified that an *E-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 an *E-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.
76. The *JFSC* is aware that a range of *E-ID* applications are commercially available for use by *supervised persons*. *Supervised persons* might also make use of *E-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 *E-ID*, or any particular *E-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 *E-ID* should be utilised in any given circumstance, and/or whether the *supervised person* will develop its own *E-ID* application for these purposes, or select an *E-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 E-ID

Statutory requirements (paraphrased wording)

77. 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** 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 that the evidence does establish that fact.

Overview

78. Using an *E-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.
79. As an alternative to using documentary evidence, Section 4.3.4 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.
80. A *supervised person* may use other tools and/or methods (including *E-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)

81. *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.*
82. *Article 15(3) 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

83. The requirements under Articles 11 and 15(3) of the *Money Laundering Order* and the *AML/CFT Codes of Practice* set out at Section 2.4.4 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 *E-ID* applications, where the *customer* is not physically present. Accordingly, when deciding whether to make use of a particular *E-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 *E-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 *E-ID* application and record the reasons why such outsourcing is appropriate
 - › consider whether the features of the *E-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.
84. 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 *E-ID* application is used, but rather when considering whether to incorporate the use of that *E-ID* application into its *CDD* measures.
85. 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.



86. The approval by a *supervised person* of the use of one *E-ID* application should not be taken to constitute approval of the use of all *E-ID* applications. It is a requirement that each *E-ID* application be risk-assessed separately and on its own merits.
87. The *supervised person* is required to ensure that adequate and effective *policies and procedures* are in place to support the use of the *E-ID* application, and are catering for the technology that is being used, as well as for the *supervised person's* business practices.
88. The *supervised person* is required to ensure appropriate training is in place.

4.3.5.2 Risks of using E-ID

Overview

89. The use of *E-ID* applications to apply *identification measures* presents a number of inherent risks. Typically, an *E-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

90. A *supervised person* may demonstrate that it has considered the particular risks that arise when using *E-ID* applications to copy documents and take photographs for *CDD* purposes when it considers the risks set out below.
91. Risk: Documents are tampered with or forged:
 - › when original documents are not physically presented, it is 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.
92. 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.
93. 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 *E-ID* application.

4.3.5.3 Factors to consider when assessing E-ID applications

Overview

94. This section lists some potential features of *E-ID* applications (and wrap-around systems) that may be used to mitigate the risks listed at Section 4.3.5.2 above. Where the *E-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.
95. 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

96. Features of *E-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).
97. Features of *E-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 *E-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 by e-mail, which presents multiple opportunities for interference
 - › a highly secure connection is used to transmit copies of documents and photographs



- › the *E-ID* application's security is regularly tested in order to guard against hacking or other security breaches.
98. Features of *E-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 in order 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 *E-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 *E-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 *E-ID* solution.

4.3.5.4 Record-keeping requirements relevant to the use of E-ID

Guidance notes

99. Where a *supervised person* uses *E-ID* applications to capture information, copy documents and take photographs of *customers* 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*.
100. Detailed *AML/CFT Codes of Practice* and *guidance notes* are provided at Section 10 of this Handbook regarding the requirements of Part 4 of the *Money Laundering Order*.

4.3.5.5 Practices or methods not considered to be E-ID

Overview

101. Whilst there are a range of *E-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 and are therefore **not** considered to be *E-ID*. Examples of these are set out in the guidance notes below.



102. 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. *E-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

103. 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 in order 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**. An *E-ID* application, or other alternative method, may be used for that purpose, enabling the independent authentication process.

104. 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 through the use of 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 an *E-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.).

105. Using a "selfie" photograph of the *customer* **without** it being biometrically compared/matched to the photograph on the identity document presented in order 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 through the use of specialist checks.

If, however, such a “selfie” photograph is being uploaded to an *E-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

106. On occasions, an individual may be unable to provide evidence of identity using the sources set out at Section 4.3.2. 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 Codes of Practice

107. 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

108. 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.

109. 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.

110. 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
- › a letter from 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 letter from 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.

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

4.3.7 Residential Address: Overseas Residents

Overview

112. 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. 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.
113. 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 Codes of Practice

114. 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.
115. 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

116. 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.
117. 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.



118. 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

119. Jersey law recognises two distinct forms of legal arrangement: the trust and the limited partnership.
120. Jersey trusts law comprises both the [Trusts \(Jersey\) Law 1984](#), 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.
121. 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 a *unit* trusts.
122. 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 into a *business relationship* or carry out the *one-off transaction* with a *supervised person* on behalf of the legal arrangement and who will be considered to be the *customer(s)*. In line with Article 3 of the Money Laundering Order, the trust or limited partnership will be considered to be the third party on whose behalf the trustee(s) or general partner(s) act(s).
123. 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), the risk factors set out in Section 3.3.4.1 and Section 7.15.1 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* (Section 6) may provide additional comfort that relevant and up to date information on identity has been found out.
124. 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). However the investors may in certain circumstances be considered *beneficial owners and controllers* and are *customers* of the Fund (see Section 13).
125. 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 Section 12 and Section 13.
126. The provisions will also assist with the identification of ultimate *beneficial owners and 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 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 or controllers.
127. 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 7 of this Handbook.
128. 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.
129. 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.
130. 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.
131. 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

132. 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 of the following components of identity:
- › name of trust
 - › date of establishment
 - › official identification number (e.g. tax identification number or registered charity or non-profit organisation number)
 - › mailing address of trustee(s).
133. 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.

134. This information may be provided by the trustee.

135. 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.

136. 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.

137. 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.

138. 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.

139. 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.

140. In any case where a settlor, protector, beneficiary, object of a power, or other person referred to in paragraphs 133 to 139 (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)(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 ((i) and (ii))
- iii) where no individual is otherwise identified under 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).



141. 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 taken into account, 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 Codes of Practice

142. 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 *JFCU* or the *JFSC*.
143. 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

144. 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

145. 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 of 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)



- › names of all general partners and those limited partners that participate in management (if any).
146. 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.
147. 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.
148. 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.
149. In any case where a partner (including a general partner) or other person referred to in paragraph 146 to 148 is not an individual, a *supervised person* may demonstrate that it has identified each individual who is that person's *beneficial owner 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 ((i) and (ii))
 - iii) where no individual is otherwise identified under 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).
150. 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 considered to be individuals who **exercise control through positions held**.



151. 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 taken into account, 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 Codes of Practice

152. 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 *JFCU* or the *JFSC*.
153. A *supervised person* must obtain evidence that any person purporting to act as general partner of a partnership which is a third party has authority to act in such capacity.

Guidance notes

154. A *supervised person* may demonstrate that it has obtained evidence under Article 3(2)(b)(i) of the Money Laundering Order that is reasonably capable of verifying that a limited partnership which is a third party to be identified is what it is said to be where the evidence covers all of the following components of identity:
- › name of partnership
 - › date and country/territory of registration/establishment
 - › official identification number
 - › registered office/business address
 - › principal place of business/operations (if different).
155. However, in the case of a lower risk relationship, a *supervised person* may demonstrate that it has obtained evidence under Article 3(2)(b)(i) of the Money Laundering Order that is reasonably capable of verifying that a limited partnership which is a third party to be identified is what it is said to be where the evidence covers the following components of identity:
- › name of partnership
 - › date and country/territory of registration/establishment
 - › official identification number.
156. A *supervised person* may demonstrate that it has obtained evidence under Article 3(2)(b)(i) of the Money Laundering Order that is reasonably capable of verifying that a limited partnership which is a third party to be identified is what it is said to be where it obtains, in every case, the partnership agreement or a copy of such an agreement certified by a suitable certifier and one or more sources of further evidence (one source for lower risk customers):
- › certificate of registration (where a partnership is registered) or copy of such a certificate certified by a suitable certifier
 - › latest audited financial statements or copy of such statements certified by a suitable certifier.



157. A *supervised person* may also demonstrate that it has obtained evidence under Article 3(2)(b)(i) of the Money Laundering Order that is reasonably capable of verifying that a partnership which is a third party is what it is said to be where the data or information comes from an independent data source (see *guidance notes* at Section 4.3.4) or (in the case of a principal place of business) personal visit to that address. An independent data source may include a registry search, which confirms that the partnership is not in the process of being dissolved, struck off, wound up or terminated.
158. Where a partner holds their role by virtue of their employment by (or position in) a business that is a *supervised Jersey trust* and company services provider, 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 trust and company services provider that the individual is an officer or employee.

4.4.5 Copy documentation provided by regulated trust and company services provider

Guidance notes

159. Where information is provided by a trust and company service provider that is regulated by the JFSC, the Guernsey Financial Services Commission or the Isle of Man Financial Services Authority (referred to in this section as “a regulated trust and company services provider”) on a person listed in Article 3(7) of the *Money Laundering Order* (following an assessment of risk in line with Paragraph 123), 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 *regulated trust and company services provider*, along with the confirmations set out in the paragraph below.
160. The confirmations to be obtained are that:
- › the *regulated trust and company services provider* 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 *regulated trust and company services provider* by a suitable certifier
 - › the *regulated trust and company services provider* is satisfied that the original document seen, or document provided to it by a suitable certifier, 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 that is held by the *regulated trust and company services provider*.
161. This will be different to a case where a *supervised person* decides to make use of Article 16 of the Money Laundering Order - which allows reliance to be placed on *reliance identification measures* that have already been completed by an *obliged person* where evidence of identity may be held by the *obliged person*, and where the *obliged person* has a continuing responsibility to the *supervised person* in respect of record-keeping and access to records - see Section 5 of this Handbook.



162. In both cases, the risk of placing reliance on an another person to have carried out *identification measures* must be considered – either as part of an assessment of *customer risk* under Article 13, or assessment of risk under Article 16 of the Money Laundering Order.
163. Nor should provision for copy documentation to be provided by a *regulated trust and company services provider* be confused with “suitable certification”, which is explained in Section 4.3.3.
164. For the avoidance of doubt this is a very limited provision applying to *regulated trust and company services providers* and does not extend to other types of *supervised business*.

4.4.6 Identification measures – Unit Trusts

Guidance Notes

165. A unit trust is defined in the Trusts (Jersey) Law 1984 (the Trust Law) as “...any trust established for the purpose, or having the effect, of providing, for persons having funds available for investment, facilities for the participation by them as beneficiaries under the trust, in any profits or income arising from the acquisition, holding, management or disposal of any property whatsoever”
166. Unit trusts are therefore primarily for investment and differ in structure from the more traditional discretionary trust. A Unit Trust may be established for different purposes, some examples of why it may be established include:
- › by someone who wishes to use it as an investment vehicle for themselves and others but wishes to share the costs as well as the profits.
 - › by an investment manager or investment bank to offer an investment opportunity to its customers.
 - › as a holding vehicle for property or other assets.
167. The settlor of a trust is defined in the Trust Law as “... a person who provides trust property or makes a testamentary disposition on trust or to a trust”. Consideration should be given as to whether a promoter/instigator/arranger is the settlor, i.e. whether they contribute property to the Unit Trust directly or indirectly. Where the promoter/instigator/arranger is not a settlor the supervised person should find out who they are to be able to adequately assess the risk of the relationship with the customer, being the Trustee of the Unit Trust.
168. While the individual investors are not considered to be settlors for the purposes of Article 3(7)(a) of the Money Laundering Order (see section 13.3.3), each of the unit holders will be customers of the Trustee (who is acting on behalf of the Unit Trust), investing their money into the unit trust. This may include the promoter/instigator/arranger as an investor. In the Trust Law a unit holders’ entitlement is described as “participation by them as beneficiaries under the trust”
169. The trustee of the unit trust is required to maintain adequate, accurate and current basic and beneficial ownership information in relation to the unit trust (see section 12.2.4.1). 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 (section 4 and section 12.2.4.1);
170. Where a supervised person (e.g., a bank or an investment adviser) 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) 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 aforementioned thresholds) sufficient information will need to be obtained about the unitholders to know who they are for the purposes of the risk assessment, customer profiles (see section 13.2.5) may be used; and
- › any other parties who exercises ultimate control over the trust, such as by other means – for example where an investment manager is the instigator of the unit trust and manages the investments of the unit trust.

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

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

Overview

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

- › companies, established under the Companies Law
- › foundations, established under the Foundations Law
- › limited liability partnerships, established under the [Limited Liability Partnerships \(Jersey\) Law 2017](#)
- › separate limited partnerships, established under the [Separate Limited Partnerships \(Jersey\) Law 2011](#)
- › incorporated limited partnerships, established under the [Incorporated Limited Partnerships \(Jersey\) Law 2011](#).
- › limited Liability Companies, established under the Limited Liability Companies (Jersey) Law 2018.

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

174. The provisions will also assist with the identification of ultimate *beneficial owners and 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) 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 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 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 or controllers*.
175. The Companies Law allows for the incorporation of cell companies: *ICCs* and *PCCs*. Each of these types of cell companies may establish one or more cells.
176. In the case of a *PCC*, each cell, despite having its own memorandum of association, shareholders and directors, as well as being treated for the purposes of the Companies Law as if it were a company, does not have a legal personality separate from the cell company. Accordingly, where a cell wishes to contract with another party, it does so through the cell company acting on its behalf. In order to ensure that creditors and third parties are aware of this position, a director of the cell company is under a duty to notify the counterparties to a transaction that the cell company is acting in respect of a particular cell.
177. Where a *supervised person* establishes a *business relationship* or enters into a *one-off transaction* with a cell of a *PCC*, because the cell does not have the ability to enter into arrangements or contract in its own name, for the purposes of Article 3 of the Money Laundering Order, the *PCC* will be taken to be a *customer* acting for a third party and the particular cell will be taken to be the third party that is a person other than an individual.
178. By contrast, in the case of an *ICC*, each cell has its own separate legal personality, with the ability to enter into arrangements or contracts and to hold assets and liabilities in its own name. Where a *supervised person* establishes a *business relationship* or enters into a *one-off transaction* with a cell of an *ICC*, the cell will be taken to be the *customer*.
179. In a case where the ownership structure of a legal person to be identified ("Legal Person A") includes other legal persons, the *beneficial owners and controllers* of Legal Person A will include those individuals **ultimately** holding a **material controlling ownership interest** in Legal Person A.
180. The *identification measures* to be applied to each type of person are set out in this Handbook as follows:
- › a company: Sections 4.5.1 and 4.5.2
 - › a foundation: Sections 4.5.3 and 4.5.4.
 - › a partnership: Sections 4.5.5 and 4.5.6.
181. For the purpose of this section, provisions that are said to apply to a company are to be taken to apply, with appropriate modification, to:
- › any other body that can establish a *business relationship* with a *supervised person* or otherwise own property
 - › an anstalt
 - › an incorporated or unincorporated association, club, society, charity, church body, or institute



- › a mutual or friendly society
- › a co-operative
- › a provident society.

182. Where information relating to a legal person is not available from a public source, a *supervised person* will be dependent on the information that is provided by the legal person. When determining the risk assessment for a legal person (Section 3.3), the risk factors set out in Section 3.3.4.1 of this Handbook will be relevant. The risk factors set out in Section 7.15.1 will also be relevant in determining whether it is appropriate to use information on a legal person provided through, for example, a trust and company services provider. In addition, the monitoring measures maintained by a *supervised person* (Section 6) may provide additional comfort that relevant and up to date information on identity has been found out.

183. Where a director of a company holds their role by virtue of their employment by (or position in) a business that is a *supervised Jersey trust and company services provider*, separate provision is made for obtaining evidence of identity. Similar provision is made for a council member of a foundation and for a partner of a partnership.

184. Article 2 of the Money Laundering Order, which describes those persons to be considered to be *beneficial owners* of a body corporate, provides that no individual is to be treated as a *beneficial owner* of a person that is a body corporate, the securities of which are listed on a *regulated market*.

185. The measures that must be applied to obtain evidence of identity of beneficiaries and persons in whose favour the council of a foundation may exercise discretion and that have been identified as presenting higher risk will necessarily reflect the verification methods that are available at a particular time to the *supervised person*. For example, it may not be appropriate to request evidence directly from a person in whose favour discretion may be exercised.

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

4.5.1 Finding out identity – Legal Person that is a company

Guidance notes

187. A *supervised person* may demonstrate that it has found out the identity of a company which is a *customer* under Article 3(2)(a) 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)
- › names of all persons holding a senior management position.



188. In order to ascertain whose identity must be found out i.e. who is/are the *customer's beneficial owner* 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 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.
189. Tier 1: A *supervised person* may demonstrate that it has found out the identity of a person who is the *customer's beneficial owner 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 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 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.
190. The above information may be provided by the company.
191. 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 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**
 - 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 company **through other means**. This effectively means that anyone exercising control through ownership and anyone exercising control through other means must be identified (points (i) and (ii))
 - iii) where no individual is otherwise identified under this paragraph (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).



192. 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.
193. 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 taken into account.

4.5.2 Obtaining evidence of identity – Legal person that is a company

AML/CFT Codes of Practice

194. 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 *JFCU* or the *JFSC*.

Guidance notes

195. A *supervised person* may demonstrate that it has obtained evidence under Article 3(2)(a) of the *Money Laundering Order* that is reasonably capable of verifying that a company which is a *customer* to be identified is who it is said to be where the evidence covers all of the following components of identity:
- › name of company
 - › date and country/territory of incorporation/registration
 - › official identification number
 - › registered office address
 - › principal place of business/operations (where different to registered office).
196. 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.
197. 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 copy of such documents certified by a suitable certifier, and one or more sources of further evidence (one source for lower risk *customers*):
- › certificate of incorporation (or other appropriate certificate of registration or licensing) or copy of such a certificate certified by a suitable certifier and/or
 - › latest audited financial statements or copy of such statements certified by a suitable certifier.



198. 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) or (in the case of a principal place of business) 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.
199. 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 trust and company services provider*, 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 trust and company service provider that the individual is an officer or employee.

4.5.3 Finding out identity – Legal person that is a foundation

Guidance notes

200. 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 of 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)
 - › names of all council members and, if any decision requires the approval of any other person, the name of that person.
201. 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

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

203. In any case where a founder, guardian, beneficiary or other person listed in paragraph 201 (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 (paragraphs (i) and (ii));
- iii) where no individual is otherwise identified under 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).

204. 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*.

205. 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 taken into account.

4.5.4 Obtaining evidence of identity – Legal person that is a foundation

AML/CFT Codes of Practice

206. 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 JFCU or the JFSC.



Guidance notes

207. 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
 - › principal place of business/operations (if different).
208. 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.
209. 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 copy of such statements certified by a suitable certifier.
210. 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) 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).
211. 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 trust and company services provider*, 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 trust and company services provider that the individual is an officer or employee.



4.5.5 Finding out identity – Legal Person that is a partnership

Guidance notes

212. 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)
 - › names of all partners (except any limited partners that do not participate in management).
213. A *supervised person* may demonstrate that it has found out the identity of a person who is the *customer's beneficial owner 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.
214. 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 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 (paragraph 213 and this paragraph).
215. Where no person is otherwise identified under paragraphs 213 and 214, a *supervised person* may demonstrate that it has found out the identity of a person who is the *customer's beneficial owner 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).
216. This information may be provided by the partnership.



217. In any case where a partner or other person referred to in paragraphs 213 to 215 is not an individual, a *supervised person* may demonstrate that it has identified each individual who is that 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 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 (paragraphs (i) and (ii))
- iii) where no individual is otherwise identified under 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).

218. 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.

219. 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 Codes of Practice

220. 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 JFCU or the JFSC.

Guidance notes

221. 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
- › principal place of business/operations (if different).



222. 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.

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

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

224. 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) 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.

225. Where a partner holds their role by virtue of their employment by (or position in) a business that is a *supervised Jersey trust and company services provider*, 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 trust and company services provider that the individual is an officer or employee.



4.5.7 Copy documentation provided by regulated trust and company services provider

Guidance notes

226. Where information is provided by a trust and company service provider that is regulated by the JFSC, the Guernsey Financial Services Commission or the Isle of Man Financial Services Authority (referred to in this section as “a *regulated trust and company services provider*”) on a person who is a beneficial owner or controller of a legal person (following an assessment of risk in line with Paragraph 182), 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 *supervised trust and company services provider*, along with the confirmations set out in the paragraph below.
227. The confirmations to be obtained are that:
- › the *regulated trust and company services provider* 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 *regulated trust and company services provider* by a suitable certifier
 - › the *regulated trust and company services provider* is satisfied that the original document seen, or document provided to it by a suitable certifier, 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 that is held by the *regulated trust and company services provider*.
228. 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.
229. 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, or assessment of risk under Article 16 of the *Money Laundering Order*.
230. Nor should provision for copy documentation to be provided by a *regulated trust and company services provider* be confused with “suitable certification”, which is explained in Section 4.3.3.
231. For the avoidance of doubt this is a very limited provision applying to *regulated trust and company services providers* and does not extend to other types of *supervised business*.

4.6 Obligation to find out identity and obtain evidence: Person purporting to act for the customer

Statutory requirements (paraphrased wording)

232. 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.



233. *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 requires a relevant person to verify the authority of any person purporting to so act.*

234. *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 Codes of Practice

235. 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.

236. 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.

237. 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 takes into account 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.

4.7 Timing of Identification Measures

Statutory requirements (paraphrased wording)

Initial

241. *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.*

242. *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.*



243. *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.*

244. *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.*

245. *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.*

246. *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)*
- › *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.*

During Business Relationship

247. *Article 13(1)(c)(i) of the Money Laundering Order requires a relevant person to apply identification measures where it suspects money laundering or financing of terrorism.*

248. *In addition, where a relevant person has doubts about the veracity or adequacy of documents, data or information previously obtained under customer due diligence measures, Article 13(1)(c)(ii) of the Money Laundering Order requires that person to apply identification measures.*

Existing Customers

249. *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.*

250. *Article 13(3) of the Money Laundering Order states that “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 JFCU).*

251. Article 13(3A) of the Money Laundering Order states that an appropriate time for finding out identity (as required by Article 3(4)) 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.

252. 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

253. 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 a designated police officer or a designated customs officer*
- › *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

254. 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, in order to comply with Article 14(2) of the *Money Laundering Order*, a *supervised person* must terminate the relationship (see Section 4.8).

255. Lawyers, Accountants and certain other professional advisers will also need to consider Sections 15.5.3 and 16.4.4, which provide sector-specific concessions for those who are in the course of ascertaining the legal position for their *customer* or performing the task of defending or representing their *customer* in legal proceedings.

256. A *business relationship* is considered to be 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 the course of establishing a *business relationship*.

AML/CFT Codes of Practice

257. 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* and the *financing of terrorism* risk is effectively managed.

258. 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

259. 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 losses – e.g. where funds have been invested in a *collective investment scheme* where a forced redemption is necessary.

260. A *supervised person* may demonstrate that *money laundering* and the *financing of terrorism* 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.

261. 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).

262. Guidance as to appropriate steps to take where a *supervised person* is unable to complete *identification measures* is provided in Section 4.8 of this Handbook.



4.7.1 Timing of identification measures during business relationship – Obtaining evidence

Guidance notes

263. 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 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* or the *financing of terrorism* occurring as a result of obtaining evidence after entitlement is conferred.
264. 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.
265. 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 or the financing of terrorism occurring as a result of obtaining evidence after conferring entitlement.
266. 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.

4.7.2 Timing for “Existing Customers”

Overview

267. *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 customers will have been less effective than those to be applied in line with *FATF Recommendation 10*.
268. For the purposes of the Money Laundering Order, the meaning of existing customer depends on the sector. In the case of a *supervised business*, this means a *business relationship* established before the *Money Laundering Order* came into force on **4 February 2008** and which continues. In the case of 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.



269. For the avoidance of doubt, the *identification measures* (finding out identity and obtaining evidence) to be applied to existing customers include the collection of information that is necessary to assess the risk that a *business relationship* involves *money laundering* or the *financing of terrorism* (in line with Article 3(5) of the Money Laundering Order). This is likely to be self-evident for an existing customer on the basis that a *business relationship* will have been established on or before the dates stated in the sector-specific sections below. In the case of a *supervised business*, for example, this means on or before **3 February 2008**.
270. Except with the agreement of the JFSC (in relation to an application from the *supervised person* made on before 31 December 2014), the effect of Article 13(3A) of the *Money Laundering Order* is to require the identity of a *customer* to have been found out by 31 December 2014. There is no similar deadline for obtaining evidence of identity.
271. Once an existing relationship has been “remediated”, then 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 paragraph 268 above, on the basis that documents, data or information will have been obtained under the *CDD* measures prescribed in Article 3.
272. 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* or the *financing of terrorism*.
273. 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 Codes of Practice

274. A *supervised person* must review its “existing customer” base in order to determine a risk assessment for each customer that has still to be remediated.

Guidance notes

275. Where it does not suspect *money laundering* or the *financing of terrorism*, a *supervised person* may demonstrate that it has **found out 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 or the financing of terrorism risk or
 - › 31 December 2014 (or later date agreed with the JFSC on application by the supervised person on or before 31 December 2014).
276. Where it does not suspect *money laundering* or the *financing of terrorism*, a *supervised person* may demonstrate that it has **found out 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).



277. Where it does not suspect *money laundering* or the *financing of terrorism*, 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* or the *financing of terrorism*.
278. 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*, taking into account 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.

4.8 Failure to Complete Identification Measures

Statutory requirements (paraphrased wording)

279. *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.*
280. *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), to terminate the relationship.*
281. *Article 14(5) of the Money Laundering Order requires a relevant person to terminate a business relationship where it cannot apply on-going identification measures.*
282. *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.*
283. *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 JFCU.*

Guidance notes

284. 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.
285. 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.
286. 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.
287. 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* or the *financing of terrorism*.



288. 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.

4.9 Challenges to identification

Overview

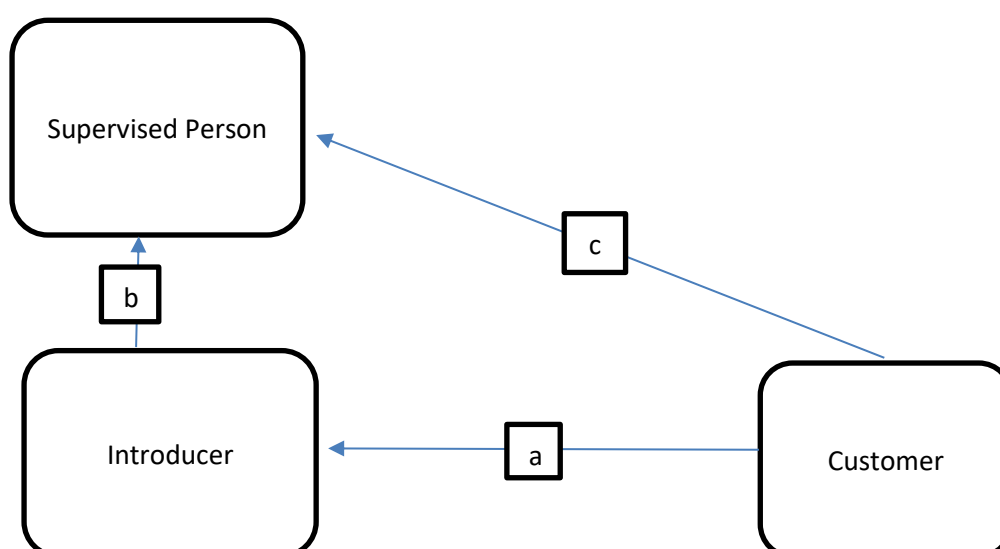
289. High net worth customers, may have their own existing framework for management of their financial affairs which may involve lawyers, accountants and other intermediaries all over the world. This can add an additional level of complexity to the customer take-on process, identification of the ultimate beneficial owner and controller and ongoing monitoring of changes to ownership and risks.

290. This section provides guidance on the following scenarios:

- › introducers/referrers
- › intermediaries/nominees/agents and
- › complex ownership structures

4.9.1 Introducers/referrers

Guidance notes



291. For the purposes of this section:

- a) the Introducer has a business relationship with the customer
- b) the Introducer introduces their customer to the supervised person



- c) the customer becomes a customer of the supervised person. The introducer may continue to act for the customer and facilitate the relationship between the customer and the supervised person or not.
292. This section relates to third party who introduces or refers a customer to a supervised person (the introducer/referrer) and is not acting as an obliged person on whom reliance is placed (see Section 5 of this Handbook).
293. A *supervised person* may be contacted by a lawyer, accountant or another introducer/referrer who may be located in another jurisdiction on behalf of their customer. This is particularly the case where a transaction has several different elements in different jurisdictions. The customer risk assessment process should include in the assessment inherent risk of the introducer. The assessment of the introducer/referrer should be a proper risk assessment with information collected, considered, assessed and the outcome documented.
294. A profile of the introducer/referrer should be created to assess and understand the inherent risk of the introducer e.g. the risk that they are introducing a customer who is attempting to conceal their involvement in money laundering. The introducer may be considered to be a professional, but this should not be accepted on face value.
295. The involvement of an introducer/referrer does not necessarily mean the risk of money laundering or financing of terrorism in the business relationship or one-off transaction is mitigated. The introducer/referrer themselves may pose a higher ML/TF risk.
296. A *supervised person* may demonstrate that the risk posed by the introducer/referrer has been considered as part of the customer risk assessment by assessing and documenting the following information (please note this list is not exhaustive):
- › Is the activity of the introducer/referrer subject to AML/CFT requirements in their home jurisdiction? FATF Mutual Evaluation Reports for the jurisdiction may have flagged that there are technical deficiencies where the AML/CFT legislative framework has not been extended fully to capture all types of DNFBPs and financial institutions
 - › Is there active AML/CFT supervision of the introducer/referrer's activity in their home jurisdiction? Mutual Evaluation Reports may cast doubts on the compliance of *supervised persons* with AML/CFT requirements due to deficiencies in the supervision of that activity
 - › How is the introducer/referrers activity/profession assessed in the National Risk Assessment of their home jurisdiction? It may indicate, for example, that those practising the activity of the introducer/referrer pose a high risk of ML/TF in that jurisdiction. For example, some may have been complicit in concealing the proceeds of crime
 - › Is the introducer/referrer part of a professional body in relation to which they are required to adopt codes of ethics, AML/CFT controls or otherwise not bring the profession into disrepute? How well does that professional body supervise these obligations? Has the introducer/referrer been subject to any disciplinary sanctions?
 - › What do external data sources (see section 3.3.4.2) reveal regarding the introducer/referrer or their profession/activities in their home jurisdiction?
 - › Consider the country risk in the context of the introducer/referrer (see section 3.3.4.1 of this Handbook). Also consider the type of business they are introducing and whether that country's National Risk Assessment indicates it is higher risk activity



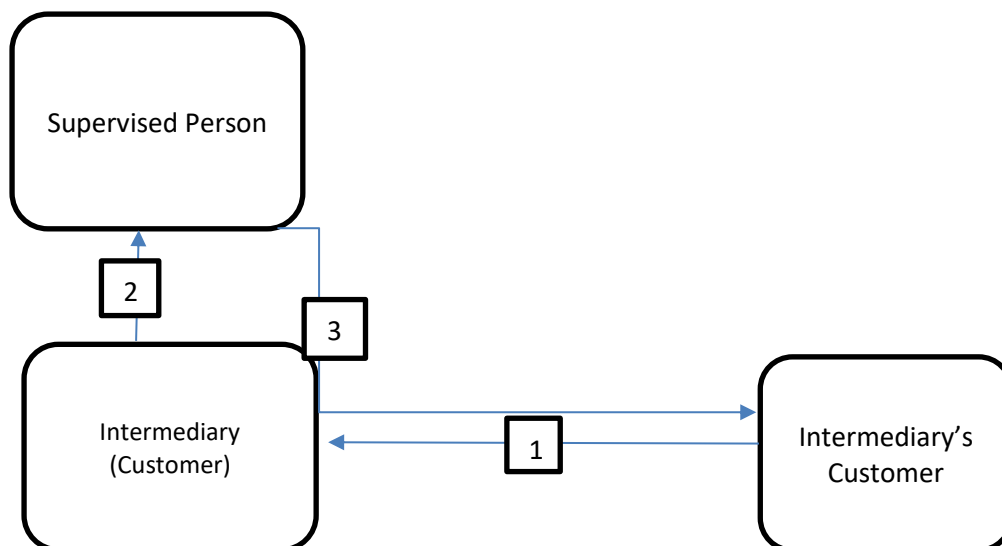
- › If a *supervised person* utilises an online tool to provide background checks, have these checks been undertaken in relation to the introducer/referrer?
297. All of this information should build into a profile of the introducer/referrer which should be risk assessed, documented and considered as part of the customer risk assessment (particularly as part of accumulation risk see section 3.3.4) when determining identification measures to apply and whether simplified or enhanced measures should be used.
298. Other relevant factors when assessing the risk of the introducer/referrer is the role the introducer/referrer plays in collation/collection of CDD re the customer:
- › Has the introducer/referrer ever met the customer?
 - › Where does the introducer/referrer get information provided to satisfy CDD requirements?
 - Directly from the customer?
 - From other third parties?
 - › Particular care should be taken where documentation is provided by the introducer/referrer to the *supervised person* which is from other third parties and additional questions may need to be asked to assess whether it is reasonable to use this information.
 - Is it reliable
 - Is it complete and accurate
 - How many third parties have provided this information
 - Who is the third party
 - Did they meet the customer
 - Is the third party a *supervised person*
 - Factors listed in paragraph 296 above may also be relevant
299. Particular care should be taken to avoid chains where documentation is passed through several parties between the customer to the supervised person. Where third parties provide material to meet the supervised person's CDD obligations this should be built into the introducer/referrers profile and risk assessment.
300. The profile and risk assessment of the introducer/referrer should be conducted at the time of taking on an introduced customer and be factored into the customer risk assessment. Consideration should be given to periodically updating the introducer/referrer's profile and risk assessment based on risk and/or at a trigger event, for instance where adverse media is identified on that introducer/referrer.
301. If the introducer/referrer regularly introduces customers, it might be appropriate to have a standalone profile and risk assessment for them which is then linked to any relevant customer risk assessment.

4.9.2 Intermediaries/nominees/agents



Guidance notes

302. This section is supplemental to and should be read in conjunction with Section 7.15 of this Handbook regarding designated relationships and pooled relationships and Section 13.3.7.



303. For the purposes of this section:

1. The Intermediary/nominee/agent has a business relationship with its customer to act as intermediary/nominee/agent.
2. The Intermediary/nominee /agent is the customer of the *supervised person* acting on behalf of the Intermediary's customer (a third party).
3. The *supervised person* provides services to the Intermediary/nominee/agent which ultimately benefit the intermediary/nominee/agent's customer (a third party).

304. Intermediaries/nominees/agents can be utilised by high-net-worth individuals to facilitate management of large portfolios of investments/holdings. This is where the Intermediary/nominee/agent is the registered owner of assets or the person with whom the *supervised person* has a business relationship. The Intermediary/nominee/agent will be subject to identification measures and risk assessment as the "customer". The Intermediary/nominee/agent may be a supervised person, such as a trust company business or an investment business, locally or in another jurisdiction. Factors may need to be fed into the risk assessment of the Intermediary/nominee/agent which are similar to those set out regarding introducer/referrers in Section 4.9.1 above.

305. A *supervised person* is required to find out if the *customer* they are acting for is acting on behalf of a third party (Article 3 (2) (b) of the *Money Laundering Order*). The person ultimately owning the third party may be at the end of a complex ownership structure (see Section 4.9.3 below).

306. It is good practice to make sure that the terms of business/engagement with any customer require them

- › to disclose if they are acting on behalf of a third party (reflecting the statutory requirement at Article 3 (2) (b) of the *Money Laundering Order*) and



- › to provide sufficient information about the third party (particularly where the third party is not an individual) to enable risk assessment and identification measures to be applied to the third party and the person(s) ultimately owning and controlling that third party.
307. An obligation to update this information should be included if there are any material changes to the third party. What constitutes a material change should be considered as part of the risk rating of the customer and third party. If there are any reduced threshold/criteria for updates from the customer this should be notified to them. The consequences of changes in ownership and control and failure to notify them to the *supervised person* should be clearly stated e.g. a transaction might not be undertaken until the correct ownership and control is established.
308. Where an Intermediary/nominee/agent is a regular customer their customer risk assessment may be undertaken, and they may be allocated a risk rating. When they act for a new third party the Intermediary/nominee/agent's customer risk assessment should be updated and be incorporate the risks of the third parties for whom they act.
309. It is also good practice to obtain a detailed ownership and control structure chart for the third party for whom the Intermediary/nominee/agent is acting. This could show:
- › jurisdictions
 - › structure type
 - › ownership percentages
 - › directors
 - › regulated parties (e.g. administrators/lenders) and
 - › any other relevant information (e.g. where there are variations within share classes).
310. An example of where a structure chart might be useful is where the third party for whom the Intermediary/nominee/agent is acting is a company with 202 shares. These shares are comprised of 200 participating shares and 2 management shares. Control of the company is attributable to the shareholder(s) holding the 2 management shares rather than the 200 participating shares.
311. The risk rating of the customer (Intermediary/nominee/agent) and third party will determine what identification measures are applied and verification information obtained.
312. Transparency of ownership is vital in ensuring that a *supervised person* is not providing services to sanctioned persons or individuals who are seeking to launder the proceeds of crime or finance terrorism.

4.9.3 Complex ownership structures

Guidance notes

313. This section should be read in conjunction with Section 13.3.6 of this Handbook and the rest of Section 4.9 above.

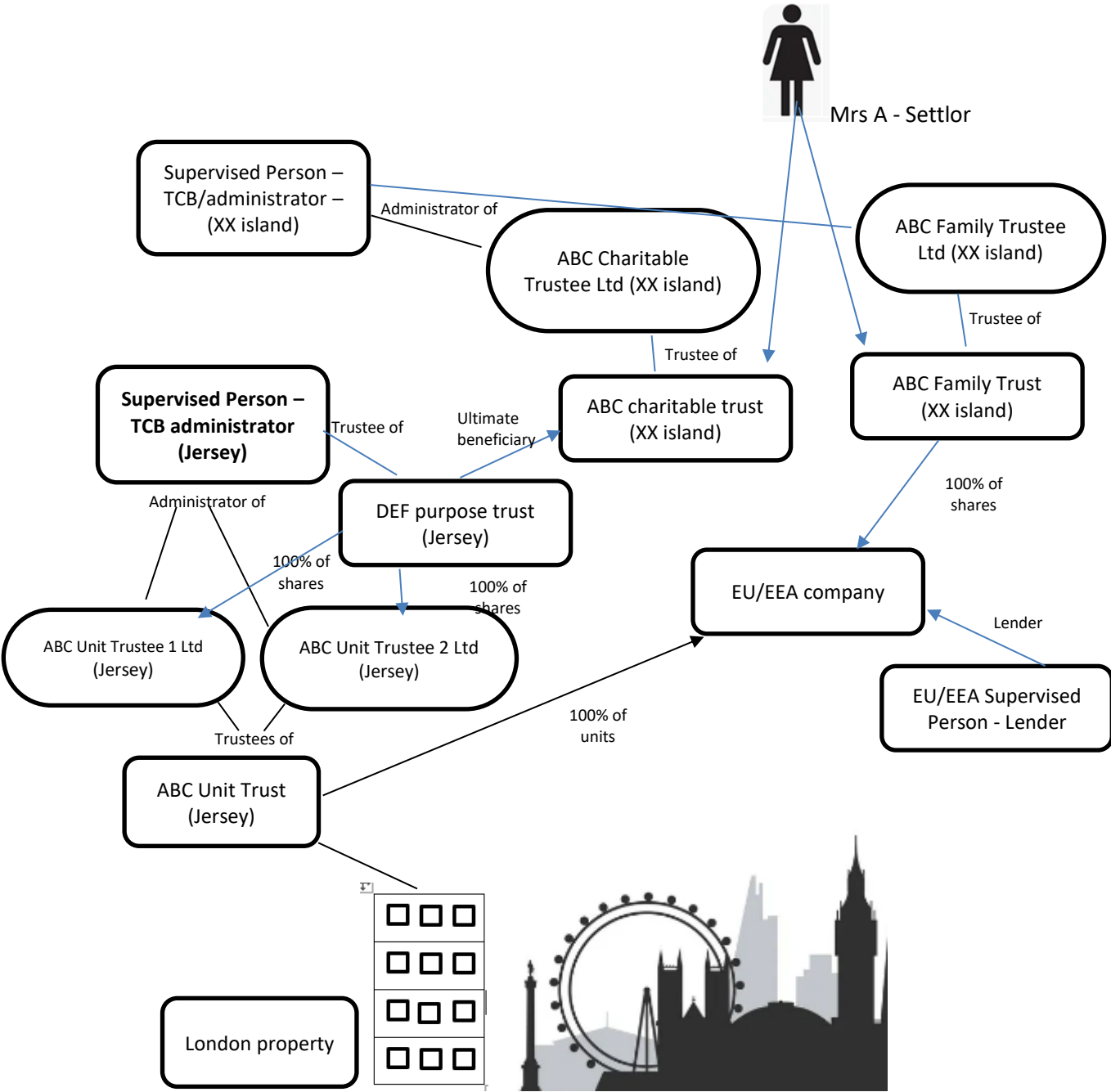


314. Customers may use complex, layered and cross-border structures to facilitate their transactions. Article 3(2)(c)(ii) of the *Money Laundering Order* requires a *supervised person*, where the customer is not an individual, to understand the ownership and control structure. A *supervised person* is required to obtain sufficient information about the structure to be able to risk-assess it, ascertain beneficial ownership and control and apply appropriate identification and risk mitigation measures.
315. The *supervised person* is required under Article 3(2)(d) of the *Money Laundering Order* to demonstrate that they understand the purpose and intended nature of the business relationship or one-off transaction. They are also required to understand the ownership and control structure of the customer and any third party for whom the customer acts.
316. To assist in complying with these requirements, the *supervised person* should demonstrate they understand the rationale behind any complex structuring. Understanding the reason for the structure will assist the *supervised person* in monitoring any transactions taking place and checking if they remain consistent with the *supervised person's* knowledge of the customer and the customer business and risk profile.
317. If the *supervised person* does not ascertain the rationale for the structure, then it will not be able to assess the risk that the structure has been created for the purpose of concealing ownership (e.g. by a corrupt or sanctioned individual) or is being used to generate/hide the proceeds of crime.
318. If changes are made to the structure, the *supervised person* should assess if this also changes the customer risk assessment.
319. In circumstances where a complex structure is present, the *supervised person* may wish to consider adopting the good practice measures referred to in paragraphs 306 to 309 above.
320. Each customer structure will need to be assessed on a case-by-case basis. If some of the types of entity involved in the structure are not familiar to the *supervised person's* staff because they are particular to a specific jurisdiction, there is a risk that ownership and control may not be understood. It may be necessary to research the structure and ask for an explanation from the customer's advisers in that jurisdiction regarding the structure.
321. Alongside ownership, the control structure needs to be understood. It may be necessary to look at the documentation establishing or otherwise creating the legal structures to ensure they are properly understood. For example, does a trust have reserved powers and if so, what powers have been reserved?
- › who are they exercised by?
 - › does it impact on the powers, control or decision making of the trustee?
 - › do identification measures need to be applied to the person(s) exercising these powers?
322. A helpful starting point once the structure chart has been obtained and initial information has been obtained is to break the structure down into different parts and consider what information documentation that will be needed. As the application of identification measures is based on risk (Article 2 (4) of the *Money Laundering Order*) it may not be possible to conduct a comprehensive customer risk assessment until after further information/documentation has been obtained. As a starting point a preliminary risk rating will need to be allocated to the *customer* (including the customer structure) with a view to reassessing the risk to fulfil the requirements of Article 3 (5) of the *Money Laundering Order* once appropriate information/documentation has been obtained.



323. The complex structure with cross-border aspects set out below is fictitious and provides an example of how a *supervised person* might approach a complex structure.

Example of fictitious Complex Structure





324. Mrs A is elderly and while originally a UK resident has moved to warmer climes for her retirement. She currently lives on XX Island, a jurisdiction which has just been added to Appendix D2 of the Handbook due to being grey-listed by FATF. Her wealth has been generated historically from her family and she has also been a successful entrepreneur in her own right, investing in projects all over the world which have significantly increased her net worth. These projects have meant that she has interests all over the world. Her family is of a globe-trotting nature and are spread throughout the world. Mrs A is concerned that as she grows older, she will not be able to actively manage her wealth and so she has set up a number of trusts.
325. She has set the ABC Charitable Trust, a purpose trust focused on innovative projects to support and promote advances in technology, and the ABC Family Trust - a discretionary trust for her ever-growing family (her 10 children, grandchildren, great grandchildren and her siblings and their children etc....) which gives her a life interest to support her and look after all her needs until her death. She does not wish her relatives to know the full extent of her wealth and their eventual entitlement, to avoid family strife.
326. Mrs A has benefitted from the advice of a number of wealth managers, legal advisers, tax advisers and accountants based in a number of jurisdictions, and she has financed her transactions to maximise the return on her investments.
327. Mrs A has been advised that she may require medical treatment and wishes to receive this in the UK. There is no indication of how long this treatment will take so her doctors are advising that it might be best for her to live in the UK for the duration of the treatment. The ABC Family Trust needs to purchase a home in central London for Mrs A. The trustees of the ABC Family Trust have decided to treat the purchase of a UK property as an investment opportunity to increase the value of the trust's assets. They have identified a block of four flats where one will be retained for use by Mrs A and her family whilst the other three will be rented out.
328. The ABC family trust has been advised that the best way to structure this transaction is to use a Jersey Property Unit Trust, owned via an EU/EEA company. The EU/EEA company will borrow money from a regulated EU/EEA lender (an EU/EEA supervised person) to fund the purchase and ring-fence liability. This EU/EEA lender offers the best rate and prefers to lend to EU/EEA companies but will want security over the units in the unit trust and the UK property. The EU/EEA company will then be owned by the ABC Family Trust. The unit trust trustees will be owned by a purpose trust (whose trustee will be the Jersey TCB *supervised person*) with an ultimate charitable beneficiary being the ABC Charitable Trust. The Jersey TCB *supervised person* is being instructed by a UK intermediary who is a lawyer acting on behalf of the Trustees of the ABC Family Trust. The provisions of the documentation to set up the EU/EEA company, the unit trust and the unit trustees are all familiar to the Jersey TCB *supervised person*.
329. The Jersey TCB *supervised person* is setting up the two Jersey Unit Trustees – ABC Unit Trustee 1 Limited and ABC Unit Trustee 2 Limited, to which it will provide the majority of the directors. The Unit trustees have been set up specifically to facilitate this transaction. The Jersey TCB supervised person will also provide the majority of the directors and be administrator for the EU/EEA company which will be formed by its EU/EEA group office. The ABC Family Trust is providing one of its trustees to be a director of each of the Unit trustees (ABC Unit Trustee 1 and 2 Ltd) and the EU/EEA company, so the ABC Family Trust has oversight of these entities.



330. The Jersey TCB *supervised person* has a long-standing relationship with Mrs A and her advisers and already have a customer profile for her. They also have introducer/referrer/intermediary risk assessments in relation to her UK lawyers, her financial advisers and the XX island TCB that is the administrator of some of her existing wealth structures. In addition, the Jersey TCB *Supervised person* currently administers a number of structures for Mrs A and have been advised as part of this transaction that the ownership of most of these structures will be transferred to the ABC Family Trust. The income and capital held in those structures will be used to partly fund the UK property purchase, along with the funds borrowed via the EU/EEA company. The grey-listing of XX Island and anticipation of this transaction has triggered an updating all these risk assessments and obtaining updated information on Mrs A's source of wealth.
331. Below is an example of good practice adopted by the Jersey TCB *supervised person*. The Jersey TCB *supervised person's MLCO (JT MLCO)* has obtained
- › an updated structure chart for before and after each of these transactions and
 - › a detailed rationale for the transactions.
332. The Jersey TCB's *MLCO* has broken down the structure chart into each of the legal structures and made notes on:
- › where it is
 - › who it is administered by
 - › whether or not the administrator is regulated for AML/CFT
 - › who the directors are and
 - › who the beneficial owners and controllers are.
333. The Jersey TCB's *MLCO* has made a list of what further information/documentation is required.
334. The Jersey TCB's *MLCO* has ascertained some information about the trusts but is awaiting sight of the final form of the trust deeds along with any updates. They have also ascertained that Mrs A is the only vested beneficiary of the discretionary ABC Family Trust and will be until she dies. It has been explained to the Jersey TCB's *MLCO* that Mrs A has over 200 family members and due to some strict conditions in the ABC Family Trust they may not all become beneficiaries. The XX Island TCB – who is the administrator of the ABC Family Trust – has a list of all the names, dates of birth and addresses for the current potential pool of beneficiaries. The XX Island TCB has also conducted online/database checks on the potential beneficiaries and their addresses but does not hold current photographic identification on all of them and will not obtain this until they have a vested interest.
335. Based on the information provided, the Jersey TCB *MLCO*, in conjunction with the Jersey TCB's board risk committee, has determined that once Mrs A's property has been settled into the ABC Family Trust it will ultimately be the trustee of that trust who is controlling the transaction. While the intermediary will remain the immediate customer of the Jersey TCB *supervised person* the legal ownership structures will alter, as will the third party for whom the intermediary acts. Therefore two engagement letters will be issued to the intermediary – one to cover the settling of the assets into the ABC Family Trust and another to cover the subsequent property transaction. The Jersey TCB risk committee and *MLCO* have allocated both transactions a preliminary inherent risk rating of high. They are taking steps to ensure all appropriate enhanced measures are applied and the risks are mitigated.



336. These steps include:

- › The Jersey TCB *MLCO* has prepared a detailed checklist of what work needs to be undertaken in terms of identification, verification and enhanced measures, along with information and documentation needed to supplement and expand the risk assessments.
- › Documented consideration has been given to:
 - the complexity of the transaction
 - the Jersey TCB *supervised person's* key administration role
 - its liability
 - the money laundering and terrorist financing risks
 - the recent grey-listing of XX Island
 - the significant value of the assets
 - the transactions involving the XX island trusts and trustees and
 - Mrs A's expectations regarding the speed of the transactions.
- › The Jersey TCB *supervised person* has decided to enter into an outsourcing arrangement with a lawyer based in XX Island to undertake the conducting of due diligence and obtaining information for the risk assessment on their behalf. The XX Island lawyer is part of a global group with an office in Jersey and the group applies Jersey AML/CFT standards. They have demonstrated a good understanding of the requirements of the *Money Laundering Order*, particularly regarding trusts, in conference calls with the Jersey TCB *MLCO* and has been provided with the detailed checklist described above. The XX Island lawyer is visiting the offices of the XX TCB administrator who provides services to the XX Island trustees and trusts (ABC Charitable Trustee Ltd and trust, ABC Family Trustee Ltd and Trust).
- › Once all the information has been obtained it will be collated by the Jersey TCB *MLCO*. The various risk assessments, including for the intermediary and the introducer/referrer, will be presented to the risk committee to be reviewed. The risk committee will reassess the risk scores, consider the enhanced measures and mitigation applied and determine if any further action is required.
- › The engagement letters will include an obligation to notify the Jersey TCB *supervised person* of material changes to the ownership and control of the structure. If it is determined that the residual risk rating of the transaction remains high the Jersey TCB *supervised person* will append the structure charts and request that it be notified of any changes in beneficial ownership and control, particularly if any beneficiaries obtain vested rights in the trusts.
- › The Jersey TCB *supervised person* will remain as administrator of the structure, which will be subject to ongoing monitoring based on risk (in accordance with the requirements of the *Money Laundering Order*). This will consist of both periodic reviews and where trigger events occur. The Jersey TCB *supervised person* has given the director provided by the ABC Family Trustee Jersey AML/CFT training which included an explanation of why the ownership and control should be updated if there are any changes.



- › As part of their periodic review process, the Jersey TCB supervised person will check that the ownership and control structure has not changed.