ISLE OF MAN
FINANCIAL SERVICES AUTHORITY

Lught-Reill Shirveishyn Argidoil Ellan Vannin

Anti-Money Laundering and Countering the Financing of Terrorism

Long term insurers

Supplemental Information Document

November 2021

Whilst this publication has been prepared by the Financial Services Authority, it is not a legal document and should not be relied upon in respect of points of law. Reference for that purpose should be made to the appropriate statutory provisions.

Version 01
(First issued November 2021)

Contents

1. Introductory

The purpose of the Supplemental Information Document for long term insurers is to provide further information to relevant persons supervised or overseen for Anti-Money Laundering and Countering the Financing of Terrorism ("AML/CFT") purposes by the Isle of Man Financial Services Authority ("the Authority"). Relevant persons must understand and satisfy their obligations under the Anti-Money Laundering and Countering the Financing of Terrorism Code 2019 ("the Code"). The Code can be found at the Isle of Man Government's legislation website. Guidance in relation to the Code can be found in the Anti-Money Laundering and Countering the Financing of Terrorism Handbook ("the Handbook"). Guidance in relation to specific sectors can be found in the sector specific AML/CFT guidance notes. The information contained in the Supplemental Information document does not have the status of guidance nor is it legislation or legal advice.

The Supplemental Information Document is not exhaustive, and does not create requirements or a checklist which must be followed. Where lists or examples are provided they are for information only, and offered to assist relevant persons in considering how they may meet their AML/CFT obligations. Each relevant person must consider its own particular circumstances on a reasonable risk basis and consider what they can do to prevent or mitigate the risks of Money Laundering and the Financing of Terrorism ("ML/FT"). This includes additional measures and controls that it may be necessary to implement in order to prevent its exploitation, and that of its products and services, by persons seeking to launder criminal property or to finance terrorism or the proliferation of weapons of mass destruction.

However, these extracts must not be considered as a substitute for the original documents. All Isle of Man primary legislation can be found here and all Isle of Man secondary legislation can be found here. The Supplemental Information Document follows the order of the Handbook.

If a term is defined in the Code the same definition applies in the Supplemental Information Document. All abbreviations used in the Supplemental Information Document, which are not otherwise used in the Code, are expanded in the AML/CFT guidance's glossary. Should any inconsistencies occur between the text in the Supplemental Information Document and the Code, the Code has primacy.

Relevant persons must note that where the term "financing of terrorism" or its abbreviation "FT" are used, they also include "the financing of proliferation" ("FP"). Accordingly where "countering the financing of terrorism" or "CFT" are used, they also include "countering the financing of proliferation" ("CFP").

The Supplemental Information Document is not the only additional source of information on ML/FT risks or on meeting AML/CFT obligations. Other sources include:

- the AML/CFT Handbook;
- sector specific guidance published by the Authority;
- the Isle of Man's National Risk Assessment published by the Cabinet Office;
- guidance and good practice provided by the IOMFIU on making suspicious activity reports;
- guidance issued by the IOMCE on Financial Sanctions, Terrorism and Terrorist Financing, Proliferation and Proliferation Financing and Trade Based Money Laundering;
- guidance issued by the Financial Action Task Force ("FATF") on ML/FT risk;
- guidelines on AML/CFT matters including on customer due diligence ("CDD") issued by the Bank for International Settlements Basel Committee on Banking Supervision; and
- guidelines on risk factors issued by the European Supervisory Authorities.

2. General requirements and risk based approach

There is no supplemental information associated with this chapter of the Handbook.

3. Customer due diligence, ongoing monitoring and enhanced measures

3.1 Introduced business

Code 9

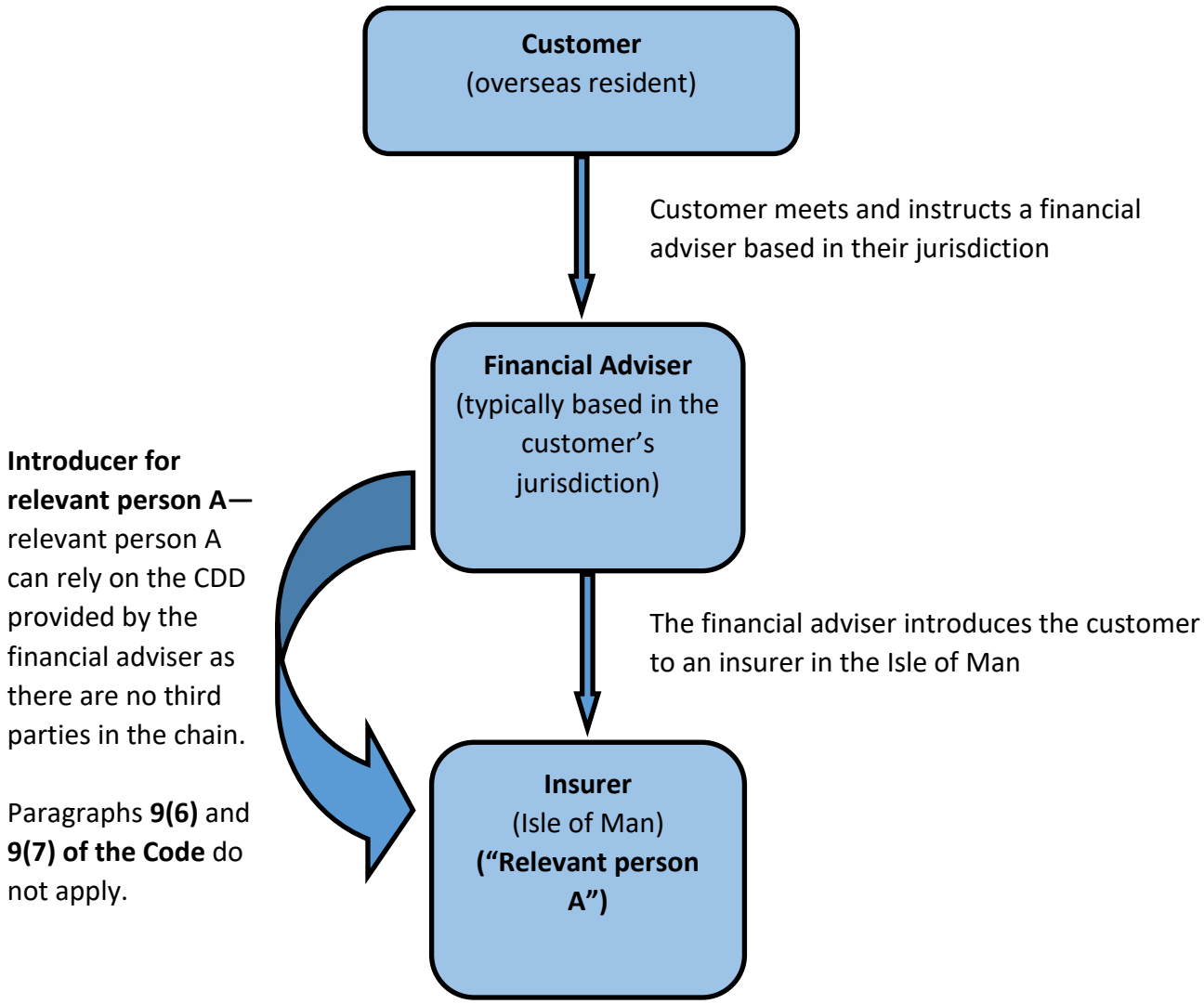
Where an introducer, who is providing elements of the customer due diligence to an insurer, is present in the relationship it is necessary to refer to paragraph 9 (Introduced Business) of the Code. It must be determined how many third parties are in the "chain" between the insurer and the customer which must form part of a broadened customer risk assessment as required by the Code.

Considering the business model which is prevalent in the sector, there would usually tend to only be one introducer involved as shown in the diagram overleaf. If there is more than one introducer in the chain between the customer and the insurer there are additional steps that are required by paragraph 9 of the Code in order to continue to use the introducer. The additional steps are explained in the Handbook at section 2.2.10 and must be followed instead of using the measures included at section 3.1 and 3.2 of the AML/CFT sector guidance for long term insurers.

Below is an example scenario for the insurance sector written to aid with interpretation of paragraphs 9(6) and (7).

3.1.1 Typical Scenario

A customer who is an overseas resident meets and instructs a financial adviser, who is typically based in their jurisdiction, in relation to wishing to purchase an insurance product. The financial adviser introduces the customer to an insurer based in the Isle of Man *(relevant person A).* The insurer can rely on CDD and verification of identity provided by the financial adviser as the financial adviser is the introducer to the insurer and there are no third parties in the chain.



3.2 What information to verify

Code 8, 11,, 12, 15

It is a matter for relevant persons to decide what specific pieces of identity information to verify on a case by case basis relative to the materiality and risk of

ML/FT with regard to their business, customer and technology risk assessments. The following are suggestions of the different pieces of identity information to verify for the more common categories of customers. For details of other customer types please see section 3.3.7 of this document.

3.2.1 Natural persons

In the case of natural persons, verification of identity could include:

1) Verification of identity information:

   For all customers:
   (i) name;
   (ii) date of birth;

   For standard and higher risk customers:
   (iii) place of birth and / or nationality;
   (iv) an official personal identification number; and

2) Verification of permanent residential address[1] (including postcode if possible).

3) Verification of identity and address of other persons per paragraph 12 of the Code.

3.2.2 Legal arrangements

In the case of legal arrangements, verification of identity could include:

1) Verification of identity information:
   (i) name;
   (ii) date of establishment;
   (iii) official identification number; and

2) Verification of addresses:
   (i) the mailing address(es) of trustee(s) (or other person controlling the applicant); and

3) Verification of the identity and address of other persons per paragraph 12 of the Code.

3.2.3 Foundations

In the case of foundations, verification of identity could include:

[1] If a different address is used for correspondence with a customer, for example a PO Box address, the relevant person should be comfortable in relation the rationale of using that correspondence address, and the validity of the address, particularly if sending any personal documentation to that address.

1) Verification of identity information:
   (i) name;
   (ii) date and country of establishment; and
   (iii) official identification number.

2) Verification of addresses:
   (i) address; and
   (ii) address of the principal place of business where this is different to the registered office/business address.

3) Verification of the identity and address of other persons associated with the legal person per paragraph 12 of the Code.

3.2.4 Legal persons

In the case of legal persons, verification of identity could include:

1) Verification of identity information:
   (i) name;
   (ii) date and country of incorporation ; and
   (iii) official identification number.

2) Verification of addresses:
   (i) registered office address/business address; and
   (ii) address of the principal place of business where this is different to the registered office/business address.

3) Verification of the identity and address of other persons associated with the legal person per paragraph 12 of the Code.

3.3 Examples of methods to verify identity and address

3.3.1 Example methods to verify the identity of a natural person

Code 8, 11, 12, 15

The examples of methods to verify identity and address of customers, and other persons per Code paragraph 12, are not exhaustive, nor should they be considered limited. It may be that, according to the relevant person's circumstances and the results of their risk assessments, more information, documents or data is required to ensure they effectively manage and mitigate their ML/FT risks. Relevant persons should establish their own lists of the source documents, data and information they will accept in each case bearing in mind the principles and considerations set out in the Handbook.

Example method	Considerations
Passport	
National identity card	These forms of documentation do not always verify nationality or place of birth. Therefore care must be taken to ensure appropriate verification of nationality and / or place of birth takes place for the customer if required. A further document may need to be obtained from the customer to verify this information where it is deemed necessary as part of a risk based approach
Provisional or full driving licence	
Known employer ID card	
Proof of age card	
Birth certificates	
International driver's permits	Caution should be exercised regarding International Driver's Permits/International Driver's Licenses. These can be obtained from unauthorised and unscrupulous operators on the internet who do not conduct any identification checks on the applicant for the Permit/Licence, and are marketed, for example, as a means of falsifying identity, avoiding driving fines and bans, and avoiding taking a driving test. International Driver's Permits can be genuine documents, but only when issued by competent national authorities to the holder of a valid domestic driving permit (i.e. national full driving licence) issued for use in the country of residence. The permit effectively converts a national licence into one for international use in other countries where the national licence is not recognised. An International Driver's Permit is not a stand-alone document.
The following additional checks may also be useful depending on the risk assessments:	
Require payment for the product or service to be drawn from an account in the customer's name at a regulated credit institution	
Independent data sources, including electronic sources	

3.3.2 Example methods to verify a natural person's address

Table 1 below sets out examples of the most reliable methods for verifying a natural person's address. Table 2 sets out other verification methods which may not, in isolation, provide the same level of confidence. Consideration should be given to whether the method used for verification provides suitable verification for all customers it is being provided for.

Table 1: Most reliable address verification methods

A recent account statement from a regulated bank, building society or credit card company
A recent mortgage statement from a regulated lender
A recent rates, council tax or utility bill (not including a mobile telephone bill)
Correspondence from an official independent source such as a central or local government department or agency in a List C jurisdiction
Photographic driving licence or national identity card containing their current residential address
The following additional checks may also be useful depending on the risk assessments:
Make a physical validation by: • Making a telephone call to the customer with a telephone number that has been independently verified as belonging to the address in question; or • Sending a letter by registered post or courier to the address in question requiring the customer to respond with a signed confirmation of receipt or confirm to the relevant person a password or code contained in that letter.

Table 2: Other address verification methods

Lawyer's confirmation of a property purchase or legal document recognising title to the property.
Tenancy agreement
Checking a phone directory
A letter from a known nursing home or residential home for the elderly confirming residence of the customer
A letter from a director or manager or a copy of a contract from a known Isle of Man employer that confirms residence at a stated address, and indicates the expected duration of employment. In the case of a seasonal worker, the worker's residential address in their country of origin should also be obtained and, if possible, verified
A letter from a person of sufficient seniority at a known university or college that confirms residence at stated address. The student's residential address in the Isle of Man should also be obtained
A letter from a director or manager (including a person from the HR Department) of a verified known employer that confirms residence at a stated address (or provides detailed directions to locate a place of residence) and expected duration of residence if known
A letter of introduction confirming residential address from a trusted person (as defined in the Code) addressed to the relevant person. The trusted person must be able to confirm they have obtained and verified, or re-verified the individual's address information recently

The following additional checks may also be useful depending on the risk assessments:
Make a physical validation by: • Making a telephone call to the customer with a telephone number that has been independently verified as belonging to the address in question; or • sending a letter by registered post or courier to the address in question requiring the customer to respond with a signed confirmation of receipt or confirm to the relevant person a password or code contained in that letter.
Independent data sources, including electronic sources.

3.3.3 Example methods to verify legal arrangements

This section sets out examples of methods to verify the identity and address of legal arrangements.

Trust Deed (or relevant extracts of the trust deed) and any subsequent deeds of appointment and retirement (or equivalent)
Bank statement (if applicable)
The following additional checks may also be useful depending on the risk assessments:
Require payment for the product or service to be drawn from an account in the customer's name at a regulated credit institution
Use independent data sources, including electronic sources
Consider obtaining sight of the letter of wishes, or other relevant documents of the trust, to confirm the beneficiaries / potential beneficiaries to the trust

3.3.4 Example methods to verify foundations

This section sets out examples of methods to verify the identity and address of foundations.

Foundation instrument (or relevant extracts of the foundation instrument)
Bank statement (of applicable)
The following additional checks may also be useful depending on the risk assessments:
Require payment for the product or service to be drawn from an account in the customer's name at a regulated credit institution
Independent data sources, including electronic sources

3.3.5 Example methods to verify legal persons

This section sets out examples of methods to verify the identity and address of legal persons.

Certificate of Incorporation Memorandum (and / or Articles of Association) Equivalent document to the above (i.e. foundation charter)
Bank statement or utility bill
Latest Annual Return
Audited financial statements which displays the company name, directors and registered address
Prepared accounts by a reporting accountant which displays the company name, directors and registered address
Conducting and recording an enquiry by a business information service
An undertaking from a reputable and known firm of lawyers or accountants confirming the documents submitted
Undertaking a company registry search, including confirmation that the institution has not been, or is not in the process of being dissolved, struck off, wound up or terminated
The following additional checks may also be useful depending on the risk assessments:
Require payment for the product or service to be drawn from an account in the customer's name at a regulated credit institution
Independent data sources, including electronic sources

3.3.6 Example methods for verifying the natural persons with the power to direct a customer

Code 12

This section sets out examples of methods for verifying the identity of natural persons with the power to direct a customer. Not all information required to be obtained or verification needed may be provided by these documents. Consequently, relevant persons may choose to use the other methods such as the examples listed in previous sections.

Obtaining a copy of signatory lists
Latest annual return
Third party authority signing mandate
Register of directors/council members

3.3.7 Different types of customer

The following provides some examples of methods for identifying (and verifying where appropriate) different types of customers insurers may enter into a business relationship with.

3.3.7.1 Partnerships/Unincorporated businesses business relationships

Measures that will produce satisfactory identity (and verification where required) of a partnership/unincorporated business as listed below include obtaining:

(a) details of the nature of the partnership/business;

(b) evidence of the trading address of the partnership/business, and, if this is not the address on the application evidence satisfactory to the insurer that the customer is resident at that address and the reasons for that address being used; and

(c) the latest annual report and set of accounts (if available).

In relation to identification and verification of identity of controllers/ partners and signatories (where applicable) please see sections 3.4.5 and 3.6.2 of the Handbook.

3.3.7.2 Limited liability partnerships business relationships

Limited liability partnerships should be treated as legal persons for identification purposes. The Code sets out how to identify a legal person (and verify where required). Please see section 3.5.4 of the Handbook and section 3.2.4 and 3.3.5 of this document for further details.

In relation to identification and verification of identity of controllers/ partners and signatories (where applicable) please see sections 3.6 of the Handbook.

3.3.7.3 Pension business relationships – occupational schemes

Where the customer is the trustee of an occupational retirement arrangement the following should be considered:

(a) That the trustees have been identified and verified in accordance with the appropriate requirements of the Code and considering the associated guidance in relation to legal arrangements at section 3.5.2 of the Handbook. Where a trustee who has been verified is replaced, the identity of the new trustee must be verified before they are allowed to exercise any control over the assets;

(b) any scheme administrator has been identified and verified in accordance with the appropriate requirements of the Code. Where a scheme administrator who has been verified previously is replaced, the identity of the new scheme administrator must be verified before they are allowed to exercise any control over the assets;

(c) satisfactory evidence of proper appointment of the trustees (and scheme administrator) has been received e.g. extracts of the deed of trust;

(d) the source or origin of the assets under the trust is known and the insurer considers it satisfactory;

(e) the trustees (and/or scheme administrators) have provided details of the parties to the trust at the time the application was made. These will typically include:

- the sponsoring employer and members of the scheme. The details of members must include the full name(s), dates of birth and current addresses;
- where the beneficiaries are named the trustee must list each. The details of beneficiaries must include the full name(s), dates of birth and current addresses of any individuals;
- where the beneficiaries are not individuals, the details of beneficiaries must include sufficient information to identify any class, corporate entity, charity or other beneficiary; and
- where the beneficiaries are disclosed as being a group of employees of the sponsoring employer this may be considered sufficient. Where a class of beneficiary other than employees of the sponsoring employer is disclosed the insurer must satisfy itself that the class does exist and undertake whatever steps it considers necessary to achieve this.

In any event an insurer must verify the identity of a beneficiary, should a payment by the insurer be made directly to that beneficiary, or for the benefit of a beneficiary, be requested by the trustees (whether named on the original list provided by the trustee, subsequently added, or included originally only by class). Detail of the Code requirements in this area are covered further in section 5.4 of the AML/CFT sector guidance in respect of long term insurers.

In relation to identification and verification of identity of controllers/partners and signatories (where applicable) please see section 3.6 of the Handbook.

3.3.7.4 Pension business relationships – non occupational schemes

Where the customer is a trustee of a retirement benefit scheme which is not an occupational retirement arrangement, for example where a scheme is a private or personal pension scheme, a retirement annuity trust scheme, a group personal pension scheme, or a small self-administered scheme , it should be considered whether:

- the trustees have been identified and verified in accordance with the appropriate requirements of the Code and considering the associated guidance in relation to legal arrangements at 3.5.2 of the Handbook. Where a trustee who has been verified is replaced, the identity of the new trustee must be verified before they are allowed to exercise any control over the assets;
- any scheme administrator has been identified and verified in accordance with the appropriate requirements of the Code. Where a scheme administrator who has been verified previously is replaced, the identity of the new scheme administrator must be verified before they are allowed to exercise any control over the assets;
- satisfactory evidence of proper appointment of the trustees (and scheme administrator) has been received e.g. extracts of the deed of trust;
- the source or origin of the assets under the trust is known and the insurer considers it satisfactory; and
- the trustees (and/or scheme administrators) have provided details of the members of the scheme. These will include the full name(s), dates of birth and current addresses of all members, and sufficient information to identify any other class, corporate entity, charity or other beneficiary.

In any event an insurer must verify the identity of a beneficiary, should payment by the insurer directly be to that beneficiary, or for the benefit of a beneficiary, be requested by the trustees (whether named on the original list provided by the trustee, subsequently added, or included originally only by class). Detail of the Code requirements in this area are covered further in section 5.4 of the AML/CFT sector guidance in respect of long term insurers.

In relation to identification and verification of identity of controllers/partners and signatories (where applicable) please see section 3.6 of the Handbook.

3.3.7.5 Pension business relationships – non trust arrangements

Where a pension scheme which is not in trust is the customer the parties to the scheme must have their identity verified as appropriate as set out in the Code and explained further in section 3.6 of the Handbook.

3.4 Suitable certifier regime

In certain circumstances relevant persons may obtain verification of identity from the customer directly, however often a third party such as a suitable certifier will be involved in the process.

3.4.1 Certification of verification of identity documents

Where copies of documents have been obtained specifically for an application, or have been requested by an insurer in relation to an existing policy (other than copy documents provided by an introducer from their records), all copy documents should be currently valid, or in the case of a utility bill or other dated document, should ideally be a recent document i.e. usually dated within 6 months.

For the certification to have value in the CDD process, the certifier should sign and date the copy document (printing their name clearly in capitals underneath) and clearly indicate their position or capacity on it and provide contact details. If the document contains a photograph, the certifier should check the photograph represents a good likeness of the customer and should also state that it is a true copy of the original. There is no exact wording to use, however the relevant person should ensure it covers the aforementioned areas.

Alternatively, the certifier may complete a covering letter or document, which is then attached to the copy identification document(s) i.e. the certification is not written on the copy identification document itself. This is suitable as long as the covering document contains the information specified in the paragraph above, and it is clear in the letter itself that it refers to the attached document.

Relevant persons should ensure that any certified documents they have received are accurate and up-to-date and recently certified. Relevant persons should also consider the clarity and legibility of hard copy documents, including the clarity of security features such as holograms, stamps and watermarks.

If the certification is carried out using different wording, or by an alternative certification method, the insurer should make a decision on whether to accept the certification based on the risk profile of the application. In these circumstances, the decision to accept the certified documentation should be documented with the relevant rationale explained.

3.4.2 Examples of suitable certifiers

This section sets out some examples of suitable persons that insurers may use to certify documents who are generally viewed as known and trusted members of the community:

- an employee of the insurer, or any group company of the insurer, which is regulated or supervised for AML/CFT purposes;
- an appointed representative, who is an individual, bound by contract to the insurer, or any group company of the insurer;
- an authorised representative of an embassy or consulate of the country who issued the identification document;
- a notary public, commissioner for oaths, lawyer or advocate, other formally appointed member of the judiciary, registrar or other civil or public servant authorised to issue or certify copy documents, or serving police officer;
- an accountant who is a member of a relevant professional organisation, which imposes on its members a requirement to abide by AML/CFT requirements;
- a director or manager of a financial institution which is regulated or supervised for AML/CFT purposes;
- an authorised employee of an agency or company[2] specialising in obtaining verification of identity documentation;
- an authorised employee of an entity that meets the Code definition of "acceptable applicant";
- an authorised employee of a regulated introducer (whether or not a terms of business is in place);
- an individual employed by an introducer who is not a regulated introducer, and who has been approved in writing by the insurer to act as a suitable certifier, subject to section 3.4.3 of this document;
- an individual within a master agent or master distributor of the insurer who has been approved in writing by the insurer to act as a suitable certifier subject to section 3.4.3 of this document;
- a registered schemes administrator under the Retirement Benefits Schemes Act 2000;
- an authorised representative of the sponsoring employer for an occupational pension only; or
- a person who is considered suitable to carry out such a function by a senior manager of the insurer. Where this option is utilised, the reason that the person is considered acceptable should be documented, including the reasons that reliance may be placed on their validation of the documents and any method which has been used to verify the identity of the suitable certifier, and signed-off by a senior manager of the insurer.

Persons acting as a suitable certifier, as described in the final bullet point above, will normally be persons who would be governed in their professional activities by AML/CFT requirements, or who would be used for the certifying of documents

in their normal occupation, and who may reasonably be considered to understand the implications of a false declaration.

3.4.3 Appointment of a suitable certifier within an introducer who is not a regulated introducer

This section relates only to the appointment of individuals within introducers who do not fall within the definition of a regulated introducer.

Only individuals can be appointed as suitable certifiers within an introducer and the position is non-transferable. There may be several employees within an introducer appointed as suitable certifiers. If an individual is a suitable certifier for one insurer that individual is not automatically a suitable certifier for any other insurer.

For the avoidance of doubt, it is possible for an introducer to have a terms of business with an insurer without any employees being suitable certifiers. When this is the case any copy documents provided to the insurer should be certified by an appropriate suitable certifier utilising the detail provided above.

Before appointing an individual of an introducer as a suitable certifier the insurer should have in place a current terms of business with the introducer. Should the terms of business be cancelled or suspended for any reason the appointment of the suitable certifier(s) within that introducer will also be terminated or suspended.

An insurer should have verified the identity of any suitable certifier. The insurer should hold a specimen signature of the suitable certifier on file and should have procedures in place to review the signatures certifying the identification documentation produced, on a regular basis to ensure their veracity.

The appointment of a suitable certifier should be documented and contain the following:

- the name of the introducer;
- details of their obligation to provide original or suitably certified copy documents which verify the identity of the customer and other parties to an application as appropriate, introduced to the insurer, sufficiently to comply with the requirements of the Code taking into account what is included in the AML/CFT sector guidance for long term insurers;
- the date from which the appointment as a suitable certifier is effective;

- any specific instructions from the insurer as to the form of words to be used when certifying the documents as true copies of the originals;
- the circumstances under which the suitable certifier status will be terminated; and
- any other provisions which the insurer wishes to impose.

3.4.4 Verification of identity by a related party

Where an employee, partner or principal of a regulated introducer is the customer, either personally or in the role of an individual trustee or nominee, they should not act as a suitable certifier to verify the identity of either themselves or of other parties or documentation relevant to the application. Any certification of copy documents should be completed by a third party.

3.5 Electronic methods to verify identity and address

The below table provides various methods relevant persons may wish to utilise in the verification of identity and address. This list is not exhaustive.

There are numerous factors a relevant person may consider when assessing the suitability, reliability, and integrity of the various methods which could be utilised to verify identity and address, many of which may be applicable across all the methods listed in the below table.

The Authority has identified these overall considerations as:

- comparison of a document to a genuine template document;
- legibility of key data on documents;
- clarity of image(s) / photograph(s);
- clarity of security features such as holograms, stamps, and watermarks;
- vulnerability to tampering of certain file types; and
- method of receipt and security of method, for example via email, or through an online portal.

Method	Considerations
Electronically certified identity / proof of address document	• Must be certified using a secure electronic system • Relevant persons must satisfy themselves of the reliability and veracity of the system prior to accepting documents certified in this way • Certifier must have seen the hard copy document in order to certify the copy is a true copy of the original • Suitability of certifier • Affiliation / registration of system with a trust service or oversight provider e.g. eIDAS • Registration of system with local data protection regulator / information commissioner
Scanned copy of a document certified in hard copy	Suitability of certifier
Photograph of individual holding their identity / proof of address document PLUS clear scanned copy of the document	• Time stamp on photograph – current? • Clarity of photograph • Clarity of scanned copy of the document • Legibility of key data on photograph AND scanned copy
Use of a software application (“app”)	• Control of the image capture – i.e. whether this is controlled by the user or app • Control of the transmission process – i.e. whether this is controlled by the user or app • Dual authenticity to access the app / capture images / transmit (e.g. password, thumbprint) • Time restrictions on image capture – presence of the individual at the time the image is captured • Geotagging – is the individual in the expected location when accessing the app / capturing images / transmitting

	• Security of connection used to transmit images captured through the app • Video or micro-stream of photographs as a liveness check – presence of the individual at the time the image is captured • Affiliation / registration of app with a trust service or oversight provider e.g. eIDAS • Registration of app with local data protection regulator / information commissioner
Use of independent and electronic data sources	• Use of negative information sources (e.g. fraud, deceased individuals) • Use of alert data sources • Sources are required to be kept up to date • Affiliation / registration of provider with a trust service or oversight provider e.g. eIDAS • Registration of provider with local data protection regulator / information commissioner

3.6 Methods for meeting a customer

Code 5, 6, 9, 15

One method of meeting a customer is for the customer to be physically present. However, in the digital age, being physically present is not necessarily the only method of meeting a customer.

A further method of meeting a customer can include (subject to the business, customer and technology risk assessments) the use of real-time visual communication media over the internet such as full-motion video conferencing. When using such media, the relevant person/introducer or other third party should clearly see the customer's face and their image on the document used to verify identity (as per the relevant person's procedures and controls) at the same time in order to be satisfied that the identity document belongs to the customer and the customer is who they claim to be.

A non-visual medium such as a telephone call does not qualify as meeting the customer.

4. Exemptions and simplified measures

There is no supplemental information associated with this chapter of the Handbook.

5. Reporting and registers

There is no supplemental information associated with this chapter of the Handbook.

6. Compliance and record keeping

Code 30

It is a matter for relevant persons to decide what must be included in the report required by paragraph 30(2) of the Code in order to cover the points listed. The following is a suggested list of points the periodic report may include:

<u>The AML/CFT environment (30(2)(a))</u>

- changes made or proposed in respect of new AML/CFT legislation, regulatory requirements or guidance and actions that have been taken regarding these changes;
- other changes to the AML/CFT environment, for instance updates to the NRA, government enforcement actions or publications by competent authorities and details of any actions taken in relation to these;
- relevant persons who are part of a group may also wish to ensure that their senior management are made aware of any changes in respect of AML/CFT legislation and regulatory requirements and guidance which affect closely linked group companies and may have an impact on group requirements;
- changes or proposed changes to international standards or guidance in relation to AML/CFT and any actions that have been taken regarding those changes;
- the nature of actions taken by the relevant person in response to notices highlighting jurisdictions which are the subject of international countermeasures, and the measures taken to manage and monitor business relationships connected with such jurisdictions that have been highlighted as posing a higher risk of ML/FT;

<u>Internal developments (30(2)(b))</u>

- the means by which the effectiveness of the relevant person's AML/CFT systems, controls and procedures have been managed and tested;
- the number of internal disclosures to the MLRO and the number of subsequent external disclosures submitted to the FIU, any perceived deficiencies in internal or external reporting procedures, and the nature of changes proposed or implemented to address any such deficiencies;

Activities relating to compliance with the Code (30(2)(c))

- information concerning the relevant person's AML/CFT training programme for the preceding year, which staff have received training, the methods of training and the nature of the training;
- information concerning the relevant person's procedures and controls for satisfying itself of the integrity of new staff members;
- any recommendations concerning additional resource requirements to ensure effective compliance with the relevant person's statutory and regulatory obligations;

Results of any testing undertaken (30(2)(d))

- any significant compliance deficiencies identified and details of action taken or proposed to address any such deficiencies; and
- details of any failures to apply the Isle of Man AML/CFT requirements in branches and subsidiaries and the proposed remediation of any such failures.

This list is not exhaustive or limited. Whilst this list is broadly grouped in relation to the requirements of sub-paragraphs 30(2)(a) – (d) of the Code some of the examples may be relevant to more than one sub-paragraph.

7. Miscellaneous

There is no supplemental information associated with this chapter of the Handbook.