ISLE OF MAN
FINANCIAL SERVICES AUTHORITY

Lught-Reill Shirveishyn Argidoil Ellan Vannin

Trust & Corporate Service Providers

Sector Specific AML/CFT Guidance Notes

March 2022

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.

Contact:
AML/CFT Division
Financial Services Authority
PO Box 58
Finch Hill House
Bucks Road
Douglas
Isle of Man
IM99 1DT

Tel: 01624 646000
Email: aml@iomfsa.im
Website: www.iomfsa.im

Contents

1. Foreword

For the purposes of this sector specific guidance, the term Trust and Corporate Service Providers ("TCSPs") refers to a business conducting activity that would require a licence under Class 4 and Class 5 of the Regulated Activities Order 2011 (as amended).

2. Introduction

The purpose of this document is to provide some guidance specifically for the TCSP sector in relation to anti-money laundering and countering the financing of terrorism ("AML/CFT"). This document should be read in conjunction both with the Anti-Money Laundering and Countering the Financing of Terrorism Code 2019 ("the Code") and the main body of the AML/CFT Handbook ("the Handbook").

Though the guidance in the Handbook, and this sector specific guidance, is neither legislation nor constitutes legal advice, it is persuasive in respect of contraventions of AML/CFT legislation dealt with criminally, by way of civil penalty or in respect of the Authority's considerations of a relevant person's (as such a term is defined in paragraph 3 of the Code) regulatory / registered status and the fit and proper status of its owners and key staff where appropriate.

This document covers unique money laundering and financing of terrorism ("ML/FT") risks that may be faced by the sector and provides further guidance in respect of approaches to customer due diligence where it may vary across between sectors.

This document is based on the following papers published by FATF:

- The Misuse of Corporate Vehicles, including Trust and Company Service Providers (2006)
- Money Laundering using Trust and Company Service Providers (2010)
- Risk-Based Approach for Trust and Company Service Providers (2019)
- Trade Based Money Laundering: Risk Indicators (2021)
- Best Practices on Beneficial Ownership for Legal Ownership (2019)
- Concealment of Beneficial Ownership (2018)
- Trade Based Money Laundering Typologies (2012)

There is also a FATF webinar which focusses on trade based money laundering that may be of use. The webinar can be found here.

The Authority recommends that relevant persons familiarise themselves with these papers and other typology reports concerning the TCSP sector. These papers also contain a number of case studies which may be of interest.

For the purposes of this document the term "customer" is generally used, in line with the Code definition.

2.1 National Risk Assessment

The Island's National Risk Assessment ("NRA") was published in 2015 and was updated in 2020. TCSPs must ensure their business risk assessment (and customer risk assessments where necessary) take into account any relevant findings of the NRA.

Considering vulnerabilities, due to the international nature of the sector, business relationships[1] may not be face-to-face and therefore there could be the involvement of third parties[2] when gathering customer due diligence. Also, TCSPs establish and provide corporate and trust structures which can be complex in nature; this is a legitimate activity but complexity provides the opportunity to disguise beneficial ownership, the source of funds and the activities of the entities concerned. The NRA sets out the main risks and vulnerabilities in further detail.

There are existing and significant international typologies for the sector. The overall risk for ML is considered to be medium high taking into account the threats and vulnerabilities, balanced against the controls in place in the sector; the overall risk for TF is medium.

3. Risk Guidance

The TCSP industry is a broad sector and the ML/FT risks will vary for each entity based on a wide range of factors such as the type of products they supply, their customers and delivery channels. The law relating to trusts (and potentially other legal arrangements) may give rise to situations which do not fall neatly into the terminology used in the Code.

The nature of services offered by TCSPs are commercially important, but can also be seen by those involved in ML and TF as useful in layering the proceeds of crime and hiding the ownership (or trail of ownership) of value or assets.

Where TCSPs are providing services or structures they should take great care to enable and allow for transparency of ownership and beneficial ownership, and not to make such ownership more opaque.

Companies incorporated in the Isle of Man are required to comply with the Beneficial Ownership Act 2017. TCSPs should be aware of any responsibilities under the Beneficial Ownership Act 2017 where they are acting as a nominated officer, or undertaking any role or responsibility for which a nominated officer is responsible for under the Beneficial Ownership

[1] Guidance in this document in respect of business relationships is also applicable to occasional transactions.
[2] There are a number of different circumstances in which third parties may be involved the due diligence gathering process, including as introducers (paragraph 9 of the Code) or Eligible Introducers (paragraph 19 of the Code).

(Nominated Officer Exemption) (Class 4 Regulated Activity) Order 2017. Further information regarding the Beneficial Ownership Act 2017 can be found here.

The Code mandates that a number of risk assessments are completed –

- a business risk assessment (paragraph 5);
- a customer risk assessment (paragraph 6); and
- a technology risk assessment (paragraph 7).

These are key mandatory requirements under the Code, and need to contain detailed evidence to show the relevant person knows the risks faced and how the relevant person considered those risks as well as their mitigation. They are vital elements to show how a relevant person meets their Code obligations to try to prevent money laundering or terrorist financing being effected through their business.

In order to complete these risk assessments and keep them up-to-date, vigilance should govern all aspects of a TCSP's dealings with its customers, including:

- customer on-boarding;
- receipt and implementation of customer instructions throughout the relationship;
- transactions into and out of relevant bank accounts;
- ongoing monitoring of the business relationship;
- technology and security issues if there is an online element to the business relationship; and
- any outsourced or delegated services.

3.1 General Higher Risk Indicators

As with the basic elements of a risk assessment, discussed in chapter 2 of the Handbook, the following activities may increase the risk of the relationship. Just because an activity / scenario is listed below it does not automatically make the relationship high risk; the customer's rationale / nature / purpose of the business relationship etc. should be considered in all cases, in line with the obligation to try to prevent money laundering or terrorist financing being effected through the business

If a business is unable to obtain a satisfactory explanation from a customer in the event of the following situations, features, or activities, or any other features which cause it concerns, it should be determined whether this is suspicious or unusual activity. Refer to chapter 5 of the Handbook for further detail of the Island's suspicious activity reporting regime.

As stated in paragraph 13 of the Code:

13 Ongoing monitoring

(2) Where a relevant person identifies any unusual activity in the course of a business relationship or occasional transaction the relevant person must –

(a) perform appropriate scrutiny of the activity;

(b) conduct EDD in accordance with paragraph 15; and

(c) consider whether to make an internal disclosure.

(3) Where a relevant person identifies any suspicious activity in the course of a business relationship or occasional transaction the relevant person must –

(a) conduct EDD in accordance with paragraph 15 of the Code, unless the relevant person believes conducting EDD will tip off the customer; and

(b) make an internal disclosure.

This list of higher risk indicators is by no means exhaustive, and TCSPs should be vigilant for any transactions where suspicion may be aroused and take appropriate measures. Also please see the list of red flags included at 3.2.

- Where a customer is reluctant to provide normal information or provides only minimal information.
- Where a customer's documentation cannot be readily verified.
- The customer is reluctant to provide the TCSP with complete information about the nature and purpose of the relationship including anticipated account activity.
- The customer is located in or conducts business in a high risk jurisdiction.
- Transactions involving numerous jurisdictions.
- Structures involved are complex and may involve multiple jurisdictions, but may not be needed for commercial purposes or may be requested by to add anonymity or to prevent an identity being confirmed or registered (for example in a company ownership or beneficial ownership or land/property register either in the IOM or elsewhere).
- The customer is reluctant to meet personnel from the firm in person and / or uses a "front person".
- It appears that the customer engages in frequent transactions with money service businesses.
- The customer has no discernible reason for using the TCSP's services, or the person's location.
- The customer has a history of changing service providers and / or using a number of businesses in different jurisdictions.
- The customer is known to be experiencing extreme financial difficulties.
- The customer enquiries about how to close structures without reasonable explanation.
- The customer opens a structure without any regards to loss, commissions or other costs associated with that account / product.

- The customer acts through intermediaries such as other TCSPs, professional service providers, money managers or advisers, as this approach may be used in order not to have their identity confirmed or registered (for instance on a Beneficial Ownership or in a property/land register either in the IOM or elsewhere).
- The customer exhibits unusual concern with the TCSP's compliance with Government reporting requirements and/or AML/CFT policies and procedures.
- Wire transfers / payments are sent to, or originate from high risk jurisdictions without apparent business reason.
- The customer's transaction pattern suddenly changes in a manner that is inconsistent with the customer's normal activities or inconsistent with the customer's profile.

3.2 Red Flags

In addition to the above higher risk indicators, there are some factors that would automatically be "red flags" in relation to that particular relationship and would therefore usually be suspicious activity. Appropriate steps as explained in section 3 of this document, and the Code, must therefore be taken. This list of red flags is by no means exhaustive and is as follows:

- where it is identified a customer provides false or misleading information;
- where it is identified a customer provides suspicious identification documents;
- where it is identified that a customer is subject to sanctions;
- the customer does not provide the TCSP with relevant / accurate information about the nature and intended or ongoing purpose of the relationship, including anticipated transactional activity;
- the customer is secretive / evasive when asked to provide more information;
- when requested, the customer refuses to identify a legitimate source of funds or source of wealth;
- when requested, the customer refuses to supply documentation to support their stated source of funds or source of wealth;
- the customer refuses to provide details on beneficial owners or provides information which is false, misleading or substantially incorrect[3];
- the customer enquires about how quickly they can end a business relationship where it is not expected;
- where the business relationship is ended unexpectedly by the customer and the customer accepts unusually high fees to terminate the relationship without question;
- the customer appears to be acting on behalf of someone else and does not provide satisfactory information regarding whom they are acting for;

[3] TCSPs should also be aware of any responsibilities under the Beneficial Ownership Act 2017 where they are acting as a nominated officer, or undertaking any role or responsibility for which a nominated officer is responsible for under the Beneficial Ownership (Nominated Officer Exemption) (Class 4 Regulated Activity) Order 2017.

- the customer is known to have or have had criminal / civil / regulatory proceedings against them for crime, corruption, misuse of public funds or is known to associate with such persons;
- the customer is interested in paying higher charges to keep their identity secret; and
- the customer seeks a Non-Disclosure Agreement ("NDA") or similar in an attempt to encourage or persuade the TCSP not to disclose information or identity details to competent authorities or in any relevant registers.

3.3 Other risk factors specific to the TCSP sector

The following section of the guidance covers some of the risk factors specifically related to this particular sector providing additional detail where appropriate. Each scenario should be determined on a case by case basis to determine whether the matter may in actual fact, depending on the context of the relationship, be a "red flag" as described in section 3.2.

- The use of complex networks of legal arrangements and/or nomineeships and/or legal persons, where there is no apparent rationale for the complexity or it appears that the complexity of the arrangement may be intended to conceal the ownership or control arrangements from the TCSP or other parties.
- The use of complex structures that go across a number of different jurisdictions, with no apparent legitimate commercial rationale as such structures could be used to hide the identity of individuals involved.
- The customer wishes to use the client money account of the TCSP without providing an appropriate rationale.
- The customer wishes the TCSP to provide director's services or nominee shareholding services, but the client effectively retains control of the entity and there are uncertainties or difficulties in the TCSP managing and controlling the entity for which they are legally directors
- The use of trading entities, particularly where the customer retains some control and where there is difficulty in monitoring movement of goods and services.
- The use of Powers of Attorney (or similar) to facilitate conduct of business by a third party on behalf of the legal person or legal arrangement.
- The activity of legal persons and legal arrangements that may involve high value goods and / or transactions.
- Structures that are involved in higher risk activities or industries.
- Structures or customers that are involved with or connected to higher risk jurisdictions.
- Involvement of politically exposed persons ("PEPs") in structures, including where the PEP may not be the TCSP's customer.
- Customers that request cash deposits and /or cash collections.
- Customers that request split boards (i.e. boards with external directors) so that they can exercise control, without appropriate rationale and controls.

- Customers who request third party signatories on client company accounts (including themselves) without an appropriate rationale.
- Beneficial owners who wish to retain control over assets through powers delegated from the board.
- Requests for credit or debit cards issued to the beneficial owner (or other third parties).
- Contracts (negotiated by customer) not provided in original format for directors and company records.
- Use of multiple addresses where no satisfactory rationale is provided.
- Requests for non-interest bearing loans to beneficiaries or beneficial owner which are later written off.
- Settlement of property (real estate, securities or cash) into a trust from third parties without appropriate explanation.
- Activity that is not in line with the trust deed.
- Requests for payments or loans to settlors rather than beneficiaries.
- Late changes in trust arrangements or in settlors and beneficiaries (such as adding back settlors as beneficiaries of the trust).
- Discretionary loans from the trust to settlor or beneficiaries which are high value but repayment is not made or not certain (such as where the recipient is financially unable to maintain and repay the loans, or there may be some uncertainty of repayment or repayment terms are not commercially reasonable);
- Requests from beneficiaries for payments to 3rd parties with no apparent legitimate rationale.

3.3.1 Pooled client accounts

Pooled client accounts operated by a TCSP can be susceptible to being abused in the ML process because:

- payments made to a third party from a regulated TCSP's client account may be considered "trustworthy" by the recipient or recipient financial institution; and / or
- transactions may be less likely to stand out as being unusual or suspicious when mingled with transactions which may be of a high volume/high value.

As per rules 3.28 and 3.31 of the Financial Services Rule Book 2016, pooled client accounts should **only** be used where circumstances make it impractical to set up a client company or trust bank account (whether in the name of the trust, the corporate trustee or a private trust company as trustee). Where a pooled client account is utilised by a TCSP they should consider and document the rationale for using this pooled account and monitor the use of this account. Appropriate controls should be put in place to mitigate the risks associated with this service such as conducting frequent and detailed transaction monitoring, paying particular attention to higher risk indicators such as:

- funds deposited into the pooled account from an unexpected source;
- requests for deposited funds to be returned to the remitter or onward transmission to a third party; (especially if the third party recipient is not directly involved in trading or service provision with the client), and/or
- overpayment of invoices and/or fees by customers followed by a request for the overpayment to be remitted.

(These higher risk indicators are applicable to all bank accounts, but the pooling of monies may make them more difficult to identify.)

3.3.2 Conflict of roles

TCSPs should consider how to prevent, or if this is not possible, perhaps due to the size of the TCSP, manage and mitigate the potential for conflicts of interest arising. For example, TCSPs should consider if there is any conflict where the same person may be director of client companies and is also the MLRO.

3.3.3 Provision of limited services

Providing limited services to a customer (e.g. registered office or registered agent only services) may present a higher risk of ML/FT due to the lack of control by the TCSP. This type of relationship can also make the identification of the customer or their location more difficult and be used to avoid inclusion in registers in either the Isle of Man or elsewhere. Where TCSPs provide such services they must be mindful of the fact that whilst they may not be directly responsible for the actions of the customer, the Code applies in full, and hence the TCSP may be liable under the Proceeds of Crime Act 2008 for the customer's actions. The limited services which are being provided should be considered in the TCSP's BRA and the CRA of the customer.

3.3.3.1 "Split boards"

As an extension to this risk, companies or trusts with "split boards" whereby some directors or trustees are supplied by the TCSP and others are provided by the client may present a similar control risk. Appropriate controls should be put in place to mitigate the risks associated with this type of arrangement. Such controls should be documented.

4. Customer due diligence

Part 4 of the Code requires relevant persons to undertake customer due diligence and ongoing monitoring in relation to all business relationships. Chapter 3 of the Handbook provides guidance on how to identify and verify the identity of the customer in relation to both a natural and legal persons, and legal arrangements. Also, guidance on the timing of identification and verification of identity is provided. Please also see section 3.8 of the Handbook for further details on source of funds and source of wealth. For details of particular concessions which may be applicable please see chapter 4 of the Handbook.

In all cases where the requirements of Part 4 of the Code cannot be met (paragraphs 8(5), 9(9), 10(5), 12(11), 14(6), 15(8) and 19(11)) the procedures and controls must provide that –

(a) the business relationship must proceed no further; (b) the relevant person must consider terminating[4] the business relationship; and (c) the relevant person must consider making an internal disclosure.

4.1 Who is the customer?

In respect of legal persons and/or arrangements, the customer at the establishment of the business relationship would usually be the person(s) who would settle or otherwise contribute the funds or assets into the structure. The Code requirements must be followed in respect of this party to the relationship, including the requirement at paragraph 12(2)(b) to determine whether the customer is acting on behalf of another person

Once the business relationship is established and the structure is formed, for the purposes of the Code, the legal person or legal arrangement would be considered to be the customer, noting the requirements of the Code in relation to beneficial ownership and control (paragraph 12). It is for the TCSP to determine on a case by case who is the controlling party of the customer and to undertake the required parts of the Code as applicable.

Guidance regarding the requirements of paragraph 12 of the Code can be found at section 3.4.5 of the Handbook.

4.1.1 Consideration of the wider structure

When conducting a customer risk assessment paragraph 6(3)(b) of the Code requires that TCSPs consider the nature, scale, complexity and location of the customer's activities. This involves looking at the wider structure, not just the entity that that the TCSP is contracting with, and identifying and assessing the risks therein.

It also involves considering the downstream activities of arrangements where the TCSP is managing a holding company arrangement to ensure the nature, scale, complexity and location of the activities conducted by assets held by the holding company are understood and assessing the risks.

Once the business relationship has been established and ongoing monitoring (including transaction monitoring) is being conducted TCSPs should continue to consider the activities of the wider structure (including any changes to the beneficial ownership and control).

[4] In relation to a New business relationship (paragraph 8) the business relationship must be terminated.

4.2 Potential beneficiaries

Paragraphs 12(3) and (4) of the Code require that relevant persons identify and take reasonable measures to verify the identity of the beneficial owner of legal arrangements and foundations by (among other things) identifying any known beneficiaries and any classes of beneficiaries (and in respect of a class of beneficiaries, where it is not reasonably practicable to identify each beneficiary, details sufficient to identify and describe the class of persons who are beneficiaries).

Where a trust has a potential beneficiary who at best only has a hope of benefitting from the trust at the discretion of the trustees at some time in the future the TCSP should make a risk based decision on whether to identify this individual.

If the circumstances change and an individual (including a member of a class of beneficiaries) becomes likely to benefit from the trust, they should be treated as a known beneficiary, they should be identified, and reasonable measures taken to verify their identity in accordance to paragraphs 12(3) and (4) of the Code.

4.3 Making payments or loans

Paragraph 12(7) of the Code requires relevant persons to take certain steps in relation to those persons who are to receive benefit from a legal person or legal arrangement.

12 Beneficial ownership and control
(7) Subject to paragraph 21(1) and without limiting sub-paragraphs (2) to (6), the relevant person must not, in the case of a customer that is a legal person or a legal arrangement, make any payment or loan to, or on behalf of, a beneficial owner of that person or for the benefit of a beneficiary of that arrangement unless it has —

(a) identified the recipient or beneficiary of the payment or loan;

(b) on the basis of materiality and risk of ML/FT, verified the identity of the recipient or beneficiary using reliable, independent source documents, data or information; and

(c) understood the nature and purpose of that payment or loan in accordance with paragraph 13.

Payments and loans can be a key risk stage in the prevention of ML/FT, a risk based approach allows for flexibility where appropriate, firstly in respect of the extent of identification information obtained and secondly when considering verifying the recipient or beneficiary's identity. This must be considered on a case by case basis.

Where a payment or loan is being made to a known beneficiary, TCSPs should consider whether the level of identification information and verification which was obtained at outset and the CRA continues to be suitable. Where a payment or loan is made to a member of a class of beneficiaries this person must be identified and verified, on the basis of materiality and risk of ML/FT, as per paragraph 12(7) of the Code.

The Authority recognises that there may be circumstances where verification of identity may not be possible or practical (such as emergency medical expenses), and in such a case, the TCSP should take a risk based approach and document the circumstances surrounding the exception. However, the Authority would expect the TCSP to know the name of this individual.

Where trust or company owned property is being let out to a beneficiary under a formal agreement such as a tenancy or licence to occupy, or an informal agreement with the trustees, if the trust or company does not benefit from receipt of a commercial / market rate of income this should be considered a benefit the same as any distribution. The TCSP should ensure they have identified and taken reasonable measures (on the basis of materiality and risk) to verify the identity of the beneficiary or third party, as in some circumstances this type of arrangement could be used to hide the ownership of the property.

TCSPs should consider the risk of the payment or loan being made, for instance a power to benefit the settlor's children is likely to present a lower risk of ML/FT than a power to benefit a party who has no obvious family connection to the settlor. This must be considered on a case by case basis using a risk based approach.

It is important to note that a TCSP's procedures must be clear in relation to the steps to be taken on payments being made, and the procedures should demonstrate that the TCSP has appropriately considered the BRA and CRA when determining the approach in this area.

Further guidance regarding making payments or loans can be found in section 3.4.5.4 of the Handbook.

Whenever payments are made TCSPs must be mindful of requirements regarding sanctioned individuals and entities. The Isle of Man Customs and Excise Division has issued guidance regarding sanctions.

5. Private trust companies

This section of the document is relevant to those TCSPs who establish and/or provide services to a private trust company ("PTC").

5.1 Applicability of the Proceeds of Crime Act 2008

Paragraph 2(6)(a) of schedule 4 to the Proceeds of Crime Act 2008 ("POCA") states that the Code applies in the following circumstances:

> subject to sub-paragraph (13), engaging in any regulated activity within the meaning of the *Financial Services Act 2008*, whether or not an exemption specified in the Financial Services (Exemptions) Regulations 2011, as those Regulations have effect from time to time and any instrument or enactment from time to time amending or replacing those Regulations, applies to that activity;

Therefore, it is important to note that the requirements of the Code apply to any activities that are exempted from the Financial Services Act 2008. This includes, PTCs which are acting by way of business and availing themselves of the regulatory exemption for PTCs detailed in the Financial Services Exemption Regulations 2011[5].

5.2 Responsibilities

All relevant persons must comply with the Code. Any relevant persons who are exempted from the Financial Services Act 2008 but are caught by POCA (for example, PTCs) must comply with the Code in their own right and must be able to demonstrate their compliance. It is acceptable for a TCSP to provide resources for another relevant person (such as a PTC) or for work in relation to Code compliance to be delegated to a TCSP[6]. Where a relevant person delegates any aspects of AML/CFT to a TCSP the board must understand and document what services the TCSP is, and, more importantly, is not providing in relation to the relevant person's obligations under the Code.

Where a TCSP is assisting a relevant person in meeting its obligations under the Code it is the Authority's expectation that a formal arrangement is put in place between the TCSP and the relevant person. Any arrangement in place should be governed by an agreement that clearly sets out the roles and responsibilities of each entity. The agreement should also clearly document how the relevant person will monitor the work of its delegate. Delegation without oversight is not effective, all delegated activities should have some level of effective upward reporting on a regular basis.

Regardless of any outsourcing or delegation that takes place, the ultimate responsibility for ensuring compliance with the Code remains that of the relevant person.

4 Procedures and controls

[5] Single Family Offices who are not acting by way of business are not caught by Schedule 4 to POCA and therefore do not have to comply with the Anti-Money Laundering and Countering the Financing of Terrorism Code 2019; however, they must comply with the Anti-Money Laundering and Countering the Financing of Terrorism (Unregulated Trustees) Code 2018.

[6] Resources can include the adoption of the TCSP's policies and procedures, provided that consideration has been made regarding the appropriateness of this and the specific risks of that relevant person.

(3) The ultimate responsibility for ensuring compliance with this Code is that of the relevant person, regardless of any outsourcing or reliance on third parties during the process.