ISLE OF MAN
FINANCIAL SERVICES AUTHORITY

Lught-Reill Shirveishyn Argidoil Ellan Vannin

Trust Service Providers
And
Corporate Service Providers

Sector Specific AML/CFT Guidance Notes

December 2015

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

Tel: 01624 646000 Fax: 01624 646001
Website: www.iomfsa.im Email: aml@iomfsa.im

Contents

1. Foreword

Trust Service Providers and Corporate Service Providers referred to collectively as "TCSPs" are the terms used to describe relevant persons carrying out activities listed under Class 4 and Class 5 of the Regulated Activities Order 2013.

2. Introduction

The purpose of this document is to provide some guidance specifically for the TCSP sector. This sector specific guidance should be read in conjunction with the main body of the AML/CFT Handbook. It should be noted that guidance is not law, however it is persuasive. Where a person follows the Authority's guidance this would tend to indicate compliance with the legislative provisions, and vice versa.

This document will cover unique money laundering and financing of terrorism ("ML/FT") risks that may be faced by the TCSP sector and will also provide further guidance in respect of customer due diligence ("CDD") measures where a one size fits all approach may not work. Also, some case studies are included to provide context to these unique risks. The information included in this document may be useful to relevant persons to assist with their risk assessment obligations under the Anti-Money Laundering and Counter the Financing of Terrorism Code 2015 ("the Code").

This document is largely based on findings from the FATF Report on Money Laundering Using Trust and Company Service Providers October 2010[1]. The Authority recommends that relevant persons familiarise themselves with this, and other typology reports concerning the TCSP sector such as Transparency International's 2015 Report *Corruption on your Doorstep*[2] and the 2010 report Puppet Masters, by Emile van der Does de Willebois et al.

The Island's National Risk Assessment ("NRA") is being undertaken at the time of writing and this document will likely be updated in due course following the publication of the NRA findings. This update is expected to take place in 2016.

3. Risk Guidance

Guidance in relation to conducting risk assessments is provided under Part 3 of the AML/CFT Handbook. This section aims to provide further guidance to the risks generally unique to the TCSP industry.

[1] http://www.fatf-gafi.org/media/fatf/documents/reports/Money%20Laundering%20Using%20Trust%20and%20Company%20Service%20Providers..pdf
[2] http://www.transparency.org.uk/publications/15-publications/1230-corruption-on-your-doorstep/1230-corruption-on-your-doorstep

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. TCSPs should take a purposive approach to the AML/CFT legislation (i.e. consider what the legislation actually seeks to achieve). They must identify, and verify the identity as appropriate, anyone who actually has influence over the management of the vehicle. They must also identify (with verification undertaken on the basis of materiality and risk) persons who actually receive benefit from it, irrespective of the legal form of that influence or benefit.

3.1. Pooled client accounts

Pooled client accounts can be susceptible to being abused in the ML process because:

(a) 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;
(b) transactions may be less likely to stand out as being unusual or suspicious when mingled with other high volume/high value transactions.

Where a pooled client account is to be used by a TCSP (as opposed to an account in the name of the client company or "as trustee of") the relevant person should consider the rationale for use of a client 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:

(a) funds deposited from an unexpected source;
(b) requests for deposited funds to be returned to the remitter or a third party; and/or;
(c) over-payment of invoices and/or fees.

3.2 . Registered office only

Legal persons to which registered office or registered agent only services are provided may present a higher risk of ML/FT due to the lack of direct control by the TCSP. The TCSP should be aware that while it may not be directly responsible for the actions of the company or foundation, the Code applies in full, and hence the service provider may be liable under the Proceeds of Crime Act 2008 for that company or foundation's actions. Section 140 states the following:

S140 Arrangements
(1) A person commits an offence if that person enters into or becomes concerned in an arrangement which the person knows or suspects facilitates (by whatever means) the acquisition, retention, use or control of criminal property by or on behalf of another person.

(2) But a person does not commit such an offence if —

(a) that person makes an authorised disclosure under section 154 and (if the disclosure is made before the person does the act mentioned in subsection (1)) the person has the appropriate consent;
(b) that person intended to make such a disclosure but had a reasonable excuse for not doing so;
(c) the act the person does is done in carrying out a function the person has relating to the enforcement of any provision of this Act or of any other enactment relating to criminal conduct or benefit from criminal conduct.
(3) Nor does a person commit an offence under subsection (1) if —

(a) that person knows, or believes on reasonable grounds, that the relevant criminal conduct occurred in a particular country or territory outside the Island; and
(b) the relevant criminal conduct —
(i) was not, at the time it occurred, unlawful under the criminal law then applying in that country or territory; and
(ii) is not of a description prescribed by an order made by the Department of Home Affairs.

As an extension to this risk, companies with "split boards" in which some directors 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.

3.3. Hold mail relationships

Hold mail relationships are those where the customer has instructed the TCSP not to issue any correspondence to the customer's address. TCSPs should exercise due caution around such relationships, only allowing relationships to be conducted on a hold mail basis as an exception and where there are plausible and legitimate reasons. Also, the Authority would suggest that this type of arrangement is periodically reviewed (on a risk-based approach) to ascertain whether the arrangement is still required by the customer and if the rationale remains the same.

3.4. Care of addresses ("c/o")

In c/o relationships mail is being issued, albeit not necessarily to the customer's address. Again, the rationale for the customer using this service should be ascertained. There are of course many genuine innocent circumstances where a "c/o" address is used, but the Authority would expect TCSPs to monitor such relationships more closely if they believe they represent a higher risk of ML/FT. The use of this type of arrangement should be monitored and it should be periodically reviewed (on a risk-based approach) to determine whether it is still required by the customer and if the rationale remains the same.

4. Higher Risk Indicators

As with the basic elements of a risk assessment discussed under Part 3 of the AML/CFT Handbook, should any of the following features or activities which may potentially increase

the risk of a TCSP relationship apply, they should be documented and any mitigating factors should be recorded.

As with all types of risk assessment, a holistic approach should be taken and the indicators below should be taken into consideration, together with all other relevant factors. However, just because a feature is listed below, does not automatically make the relationship higher risk provided that suitable controls are in place.

1. 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 is intended to conceal the ownership or control arrangements from the TCSP or other parties;
2. complex structures that go across a number of different jurisdictions, with no apparent legitimate commercial rationale;
3. trading entities, particularly where the customer retains some control and where there is difficulty in monitoring movement of goods and services;
4. legal persons and legal arrangements that involve high value goods and / or transactions;
5. structures that are involved in higher risk activities or industries e.g. mining, oil, pharmaceuticals;
6. structures or customers that are involved with or connected to higher risk jurisdictions;
7. involvement of PEPs in the structures, including where the PEP may not be the TCSP's customer;
8. customers that request cash deposits and /or cash collections;
9. customers that request split boards (i.e. boards with external directors) so that they can exercise control, without appropriate rationale and controls;
10. customers who request third party signatories on bank accounts (including themselves);
11. beneficial owners who wish to retain control over assets through powers delegated from the board;
12. requests for credit or debit cards issued to the beneficial owner (or other third parties);
13. contracts (negotiated by customer) not provided in original format for directors and company records;
14. requests for non-interest bearing loans to beneficiaries or beneficial owner which are later written off;
15. settlement of property (real estate, securities or cash) into a trust from 3rd parties without appropriate explanation;
16. requests from beneficiaries for payments to 3rd parties with no apparent legitimate rationale; and/or;
17. customer does not provide requested information but says that he has carried out the necessary checks; Customer exhibits unusual behaviour – either is aggressive to junior staff (seeks out weakest link) or is over friendly and never queries actions or fees.

5. Customer Due Diligence

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 and the due diligence requirements under paragraphs 10 and 11 of the Code (new business and continuing business) must be followed.

Once the 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 and so paragraph 13 (beneficial ownership) of the Code takes effect. Paragraph 13 requires the TCSP to conduct due diligence on the beneficial owner(s) and controller(s) – see part 4 of the AML/CFT Handbook for further details.

The beneficial owner or controlling party of the customer would normally be considered to include:

(a) the settlor(s);
(b) enforcer or protector (or any other party to whom dispositive powers have been conferred);
(c) a principal beneficiary;
(d) any shareholder who would objectively be considered as a controlling party (looking through any nominee or parent company arrangements);
(e) the person who the TCSP has signed terms of business with under Rule 6.63 of the Financial Services Rule Book;
(f) the person who pays the TCSP's fees or gives consent for the fees to be taken or adjusted; and;
(g) the directors and signatories of a company the TCSP is providing registered office/agent services to. Where a board is particularly large, such as an international charity or listed entity, a risk based approach may be taken. Please see part 4.6 of the AML/CFT Handbook for further details on this.

Paragraph 13(5) of the Code requires TCSPs to identify and verify the identity of those persons who are to receive benefit from a legal person or legal arrangement. Set out below are some examples of possible scenarios and associated guidance on the persons to be identified and their identity verified.

(a) Beneficiaries to whom the trustees are required to distribute assets, including accumulation and maintenance settlements and interest in possession trusts. In these circumstances, because a payment must be made, the beneficiaries should be identified and their identity verified at the commencement of business and/or prior to the making of the first distribution payment (unless extenuating circumstances are present such as a beneficiary doesn't exist yet).

(b) Any known beneficiaries should be identified at the time of establishing the business relationship and verification of their identity completed prior to a payment or loan being made.

Known beneficiaries include those listed in the trust instrument or a deed of amendment of a trust which is not a discretionary trust. However, the Authority does accept 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.

Where there is a potential beneficiary who is merely an object of a power and at best only has a hope of benefiting from the trust at the discretion of the trustees at some time in the future the TCSP is not required to fully identify the potential beneficiary in line with the AML/CFT Handbook section 4.5 "How to identify".

However, where possible we would expect the TCSP to know the name of this individual (i.e. where this is not possible, for example in the case of an unborn family member, a risk based approach may be taken). If the circumstances change and this person becomes likely to benefit from the trust they should then be treated as a known beneficiary as explained above (i.e. fully identified as explained in the AML/CFT Handbook, and their identity then verified if they come to benefit from the legal arrangement).

As with any aspect of AML/CFT prevention, the TCSP should apply a risk-based approach. 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.

Where a person is to be the recipient of a loan or other benefit from a trust or corporate structure, the TCSP should identify who that person is and take reasonable measures to verify their identity (on the basis of materiality and risk) as well as the purpose of the loan and the rationale for using the trust or corporate structure rather than an alternative source.

(c) 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.

(d) A revocation of a revocable trust (either partial or full) will be considered by the Authority as a distribution. Therefore any person receiving the proceeds (be they a beneficiary, the settlor or a third party) should be identified and reasonable measures taken (on the basis of materiality and risk) to verify their identity.

(e) Paragraph 13(5) of the Code states that in relation to a legal person or legal arrangement, where a beneficial owner or beneficiary of the arrangement is receiving a payment they should be identified and their identity verified (on the basis of materiality and risk). The Authority would expect a TCSP to take a risk based approach to any distribution to a third party and to obtain sufficient CDD to satisfy themselves that they are comfortable making the payment to the third party in question.

6. Case Studies

The case studies below are real life examples where risks have crystallised resulting in actual cases of ML/FT, losses and sanctions (civil and criminal) against the TCSP and related

individuals. The case studies included in this document are based on internationally published typology documents concerning the TCSP sector.

6.1. Concealment of beneficial ownership through the use of shell companies

An employee at a lawyer's office was the administrator for 300 companies established through the law office on behalf of its client, many of whom were known to be involved in international criminal investigations. The majority of the companies were shell corporations established in an American State, although some companies were incorporated in Spain for the purpose of being used in money laundering schemes based on the real estate market. The Spanish companies were usually owned by the American shell companies and these pre-constituted companies would have been incorporated using the name of an agent, usually a lawyer.

The documents of incorporation for such companies would remain inactive in the hands of the agent until the company was bought by a client, and at the moment of purchase the company would become effective. The board of these pre-constituted companies when first registered would comprise the agent and his associates, who would usually have no link with the real owners who subsequently purchased the shell company.

(Based on an example in the 2010 FATF report *Money Laundering Using Trust and Company Service Providers*)[3]

6.2. TCSP as a facilitator of money laundering

X was a chartered accountant and the sole principal of a financial services business trading as X & Co. He acquired companies, provided directors, formed trusts and acted as trustee. He was signatory to hundreds of bank accounts. X used these facilities as a tool kit to help foreign clients to cheat their fiscal authorities and launder the proceeds of crime.

X laundered the money in a variety of ways. He extracted money from foreign trading companies using false invoices drafted at the behest of clients, holding the sums received anonymously for his clients. He layered millions of pounds through his pooled accounts. He obtained and delivered cash from and to his clients. He lied about the beneficial ownership and purpose of his companies and the origin of property to the Jersey authorities and others.

A key aspect of his business was his trade in bank notes. He obtained cash from clients who wanted to get rid of it, crediting bank accounts held for them with equivalent sums sourced from different money in return. The actual cash was then delivered to other clients who wanted their income securely returned to them in this fashion – bank notes which he personally delivered to them in Country A. These dealings were hidden by the operation of a spider's web of bank accounts.

[3] http://www.fatf-gafi.org/media/fatf/documents/reports/Money%20Laundering%20Using%20Trust%20and%20Company%20Service%20Providers..pdf

The result of these activities was that it was impossible to ascertain the origin and ownership of property without access to the records of X and Co. Even then the tracing exercise was extremely difficult, requiring years of analysis by investigative lawyers, police, and forensic accountants to unravel.

(Based on an example in the 2010 FATF report *Money Laundering Using Trust and Company Service Providers*)[4]

6.3. Stolen funds hidden in a web of corporate vehicles

In 1990 the Government of Antigua and Barbuda ("GOAB"), issued to GOAB Ambassador Bruce Rappaport the authority to renegotiation the GOAB's debt with the Japanese company Ishikawajima-Harima Heavy Industries Co. Ltd. ("IHI"). According to a civil complaint filed in Florida, by the GOAB, Rappaport manipulated the debt settlement numbers so that the GOAB in effect agreed to make overpayments to IHI Debt Settlement Co. Ltd. ("IHI Debt Settlement") – a company beneficially owned by Rappaport and that purportedly was used to administer the terms of the debt.

The IHI debt required monthly payments of only $199k to IHI for 25 years. Rappaport had allegedly manipulated the numbers so that the GOAB instead was to pay $404k on a monthly basis for 25 years. As a result of this scheme, the GOAB was deceived into making payments in excess of $14m.

From 1996 to 2003, the monthly payments were made to IHI Debt Settlement's bank account in Bermuda. After the money was received court documents showed Rappaport then funnelled the overpayments to a web of various other corporate vehicles.

(Based on an example in the 2010 report *Puppet Masters,* by Emile van der Does de Willebois et al*)*[5]

6.4. Misuse of shelf companies

IHI Debt Settlement, Dredson and Gregson were all shelf companies, IHI Debt Settlement was incorporated under the name Offshore Services Limited in 1970. It was not until 1997 that the company changed its name to IHI Debt Settlement. The other two companies – Dredson and Gregson – were both incorporated in 1970, 17 years before being named as IHI Debt Settlement's principal shareholders.

People may choose to use shelf companies for a variety of reasons. One such reason may be to create the appearance of legitimacy that comes with longevity. Another reason might be to circumvent information requirements required at incorporation. According to the then-senior counsel for the U.S. Department of Justice – criminals can easily throw investigators

[4] http://www.fatf-gafi.org/media/fatf/documents/reports/Money%20Laundering%20Using%20Trust%20and%20Company%20Service%20Providers..pdf

[5] https://star.worldbank.org/star/publication/puppet-masters

off the trail by purchasing shelf companies and then never officially transferring the ownerships. In such cases the investigation often leads to a formation agent who has long ago sold the company with no records of the purchaser and no obligation to note the ownership change.

(Based on an example in the 2010 report *Puppet Masters,* by Emile van der Does de Willebois et al*)*[6]

6.5. Misuse of trusts to disguise ownership of corporate vehicles and assets

Diepreye S.P. Alamieyeseigha ("A") was arrested at Heathrow Airport in 2005 on suspicion of money laundering offences. A search of "his" apartment (it was registered in the name of a company) revealed nearly a million pounds worth of British, European and U.S. currency, After his arrest he fled the U.K. and returned to Nigeria where he was impeached and dismissed from his position as governor of Bayelsa State. During A's initial two terms in office, it is alleged that by participating in corrupt activities, he had enriched himself by tens of millions of dollars' worth of internationally held monetary assets and property holdings, often held in the name of corporate vehicles.

A created at least five corporate vehicles that separated his name and beneficial interest from the legal ownership and control of various financial and real estate assets. Following typical trends of misusing corporate vehicles, the majority were private limited companies in a variety of jurisdictions (acquired and managed through a variety of banking and administration trust and corporate service providers.

(Based on an example in the 2010 report *Puppet Masters,* by Emile van der Does de Willebois et al*)*[7]

6.6. Misuse of trusts

In 2001 upon the advice of his bank, A settled "the Salo Trust" for the benefit of his wife and children. A later acknowledged that he was a beneficiary of the trust, but he maintained that he was initially unaware that he was himself listed as a beneficiary along with his wife and children.

The trustees of the Salo Trust either purchased or incorporated Falcon Flights Inc. pursuant to the terms of the trust agreement. In the first claim made against A and his companies in early 2007, the England and Wales High Court (Chancery Division) held that it was established by documentation that in 1999 A opened a U.S. dollar account with the bank in London with an initial deposit of $35k and a balance in 2005 of $535k attributable to various sources. The originator was often recorded simply as "Foreign Money Deposit". A states that the account funds amounted to "contributions from friends and political associates towards the education of my children" a claim that the court would later find dubious. A's defence further stated that the account's status as a trustee account led him to not list the account on the declaration-of-assets for that is required for all Nigerian governors.

[6] https://star.worldbank.org/star/publication/puppet-masters
[7] https://star.worldbank.org/star/publication/puppet-masters

The net effect of the preceding evidence was that A represented himself as or admitted to being, in various capacities, (a) the settlor, though claiming the true economic settlements came from "friends" whom he could not specifically recall; (b) the trustee, insofar as the account legally opened and controlled in his own name was held out to be a trust account; and (c) a beneficiary, a concession made by his defence.

The existence of the trust separated A from the legal and beneficial ownership and control of the assets contained therein, and added another layer of complexity to those who would have tried to discover that he did indeed hold such assets.

In addition, this account received funds in the amount of approximately $1.5m through two deposits made in 2001 by one Aliyu Abubakar, a state contactor A had met a year earlier. These deposits were immediately converted into bonds, which were then transferred to the portfolio holdings of Falcon Flights Inc., effectively burying A's claim, over the assets within a nested corporate vehicle structure.

(Based on an example in the 2010 report *Puppet Masters,* by Emile van der Does de Willebois et al*)*[8]

[8] https://star.worldbank.org/star/publication/puppet-masters