Financial Intelligence Unit

Government of the Cook Islands

Financial Transactions Reporting Act 2017 Practice Guideline for Trustee Companies

1. Introduction

The purpose of this document is to provide guidance specifically for Trustee Companies.

This document is designed to assist you with your Anti Money Laundering and Terrorist Financing (AML/CFT) obligations and should be read in conjunction with the Financial Transactions Reporting Act 2017 (FTRA), the Financial Transactions Reporting Regulations 2017 (Regulations) and the Practice Guidelines for the Financial Transactions Reporting Act 2017 (Guidelines).

It addition to the FTRA, the Regulations and the Guidelines it is recommended you refer to the following for further guidance:

- FTRA Practice Guideline for Lawyers, Notary Publics and other independent legal professionals; and
- FATF Report on Money Laundering Using Trust and Company Service Providers October 2010[1]

It should be noted these guidelines are not law and do not constitute legal advice. They should not be relied upon as evidence of you complying with your obligations under the FTRA and the Regulations. You should seek your own independent legal advice on the interpretation and requirements of the FTRA and the Regulations.

If you have any questions or require more information concerning these guidelines, the FTRA, the Regulations and the Guidelines please contact the Financial Intelligence Unit.

2. Who has obligations under the FTRA?

All trustee companies licensed under the Trustee Companies Act 2014 are, pursuant to the Financial Supervisory Commission Act 2003, licensed financial institutions. For the purposes of the FTRA all licensed financial institutions are reporting institutions and must therefore comply with the FTRA and the Regulations.

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

3. What are your obligations under the FTRA?

You must develop internal policies, procedures, controls and systems to ensure the following obligations are met:

- internal compliance programme and risk assessments under Part 2, including;
    - appointing a Money Laundering Reporting Officer (MRLO) to oversee your compliance programme;
    - training employees to be aware of the policies, procedures and audit systems adopted by your organisation to deter money laundering and the financing of terrorism;
    - screening directors and key employees before appointing them; and
    - establishing an internal review function to test the effectiveness of your compliance programme and its compliance with the FTRA.
- customer due diligence ncluding identifying Politically Exposed Persons (PEPs) and record keeping under Part 3;
- reporting of cash transactions and suspicious activities under Part 4.

Please refer to the Guidelines for further information and assistance in relation to each of the obligations mentioned above.

4. What are some of the risks specific to the trustee companies

Due to the nature of trustee company business and the services offered by trustee companies, trustee companies will always be exposed to the risks of financial misconduct, including money laundering, terrorist financing, tax evasion and corruption. Notwithstanding the best efforts of trustee companies to manage and mitigate such risks, such risks will always exist. You must therefore be vigilant in your compliance with AML/CFT laws and regulations seeking out criminals who will look to exploit your services to conceal their activity and identity. Areas you should pay close attention to include:

a) Pooled customer accounts

Pooled customer accounts (as opposed to an account in the name of the particular natural or legal person or “as trustee of”) can be susceptible to abuse in the money laundering process because:

- Payments made to a third party from a licensed trustee company, customer account may be considered trustworthy by the recipient including financial institutions; and/or
- 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 customer account is to be used by a trustee company appropriate controls should be put in place to mitigate risks associated with this service. For example controls should include conducting frequent detailed transaction monitoring, paying particular attention to higher risk indicators such as:

- funds deposited from an unexpected source;
- requests for deposited funds to be returned to the remitter or a third party; and/or
- overpayment of invoices and/or fees.

b) Registered office only

Legal persons (international companies, LLCs, foundations) to which registered office or registered agent only services are provided may present a higher risk of financial misconduct due to the lack of direct control by the trustee company over the legal person's activities and assets. Companies with "split boards" (that is where some directors/managers/council members are supplied by the trustee company and some by the customer) 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 include, in addition to obtaining customer due diligence as required by the FTRA, obtaining sufficient information on the management of the legal person and its activities and assets to provide comfort that no criminal activity exists or is intended. Such information should be updated at least annually.

c) Face to face meetings with ultimate principals

The services offered by trustee companies often result in no face to face meetings with those individuals who ultimately own or effectively control the legal person or legal arrangement and the assets held within those structures. This practice contains inherent risks of abuse by criminals therefore requiring more rigorous due diligence measures. It is expected in such circumstances that trustee companies will consider the level of risk involved and that enhanced due diligence be applied (s29 (1)(d) FTRA).

d) Use of business introducers and intermediaries

It is common for trustee companies to obtain business through business introducers and intermediaries. This practice may mean that you do not meet face to face with the ultimate principals of the legal person or legal arrangement resulting in increased risk of criminals using structures to hide their criminal activity and identity. As noted in (c) above it is expected in such circumstances that that trustee companies will consider the level of risk involved and that enhanced due diligence be applied in respect of the ultimate principals. In addition, it is expected that due diligence be carried out on each business introducer and intermediary, being a person acting on behalf of a customer (s25 (1)(b) FTRA).

e) Control of underlying assets

Depending on the structure, assets and customer requirements, a trustee company may have complete, partial or no control over assets in the structure and the activities of any legal person or legal arrangement within the structure. A trustee company having limited or no control over assets within a structure will most likely be due to the ultimate principal's desire to retain control over his/her assets but at the same time hold them out of his/her personal name and home jurisdiction. The risk of a trustee company being unwittingly involved in ML/TF or other criminal activity is greatly increased where it provides a trustee or nominee shareholder and other administration services but does not have control over assets and activities within the structure.

It is expected in such circumstances that trustee companies will consider the level of risk involved is such that enhanced due diligence be applied (s29 (1)(d) FTRA) as well as obtain sufficient information on the management of the legal person and its activities and assets to provide comfort that no criminal activity exists or is intended. Such information should be updated at least annually.

f) Hold mail relationships

Hold mail relationships are those where the customer has instructed the trustee company not to issue any correspondence to the customer's address. You should exercise due caution and ensure that there are plausible and legitimate reasons for the relationship. The use of this type of arrangement should be monitored and periodically reviewed (on a risk based approach) to determine whether it is still required by the customer and if the rationale remains the same and acceptable.

g) Care of addresses

In care of address (c/o) relationships mail is being issued but not necessarily to the customer's address. The rationale for using this service should be ascertained. There are many genuine circumstances where a "c/o" address is used but the relationship should be monitored on a risk based approach and it should be periodically reviewed.

5. High Risk Indicators

The nature of a trustee company's business means it will always be exposed to the risks of financial misconduct, including money laundering, terrorist financing, tax evasion and corruption. The following scenarios are examples intended to highlight where the risks of financial misconduct are higher requiring the trustee company to be more vigilant in its assessment of risk and the measures put in place to mitigate those risks.

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 trustee company or other parties;
2. complex structures that go across a number of different jurisdictions, with no apparent legitimate or 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, eg. mining, oil, pharmaceuticals;
6. structures or customers that are involved with or connected to higher risk jurisdictions;
7. involvement of PEPs in the structure, including where the PEP may not be the trustee company's customer;
8. customers that request cash deposits and/or cash collections;
9. customers that request board control so that they can exercise control over assets and activities without trustee company interference and without appropriate rationale;
10. customers who request third party signatories on bank accounts (including themselves) without appropriate rationale;
11. requests for credit or debit cards issued to the ultimate principal (or other third parties);
12. inability of customer to reasonably justify frequent and large asset injections into or dispositions from a trust or legal person;

13. asset injections into a trust or legal person that do not align with the trustee company's understanding of the customer's source of wealth and intended purpose and use of the structure;
14. transactions requested by the customer that are not in line with the purpose or rationale of the structure or the understood activity of a trust or legal person.
15. dormant accounts that suddenly become active without appropriate rationale;
16. requests for non-interest bearing loans to beneficiaries or ultimate principals which are later written off;
17. service contracts entered into with the customer, ultimate principal or other third party where commissions are to be paid into bank accounts outside that person's home jurisdiction;
18. settlement of property (real estate, securities, cash) into a trust from third parties without appropriate explanation;
19. requests from beneficiaries for payments to third parties with no apparent legitimate rationale;
20. customer does not provide requested information or exhibits unusual behavior.

The above list is not exhaustive. New methods for laundering money and financing terrorism are constantly being developed. Typologies reports produced by the FIU are available on the FSC's website and you should contact the FIU for the latest information where you are uncertain or have questions on any risk matter.

6. When should you conduct Customer Due Diligence?

Customer due diligence must be undertaken before entering into an ongoing business relationship or an isolated transaction with or on behalf of a customer.

In respect of legal persons or legal arrangements, the customer at the establishment of the ongoing business relationship would usually be the person(s) who settles or otherwise contributes funds or assets into the structure and due diligence requirements under Part 3 of the FTRA must be followed. It is important to note you must also undertake due diligence on any person acting on behalf of a customer.

Once a relationship is established and the structure is formed, for the purposes of the FTRA, the legal person or legal arrangement would be considered to be the customer and you must ensure the requirements of Part 3 of the FTRA are met. This includes identifying and verifying any ultimate principals.

In addition, the Regulations at regulation 6 also requires you to identify any controlling party of a legal arrangement or foundation and its beneficiaries. Beneficiary due diligence requirements include:

- beneficiaries with a vested interest in the assets of the legal arrangement or foundation (unless more than 10 in number). Because a payment must be made, the beneficiaries should be identified and their identity verified at the commencement of business, unless extenuating circumstances are present such as a beneficiary does not yet exist.
- potential beneficiaries who are merely an object of a power and at best only have a hope of benefiting from the trust (e.g.a discretionary trust) at the discretion of the trustees or foundation council at some time in the future. As no payment is fixed or certain, the trustee company is not required to identify the beneficiary but must instead obtain sufficient information about the class of beneficiaries or characteristics of the beneficiary to enable identification and verification of that

beneficiary before any distribution is made. This also applies to charitable trusts and foundations as well as trusts and foundations that have 10 or more beneficiaries.

The law relating to legal arrangements (trusts), foundations and similar arrangements may give rise to situations which do not fall squarely within the provisions provided by the FTRA or the Regulations. You, as a reporting institution, should take a purposive approach to the FTRA and the Regulations and consider what the legislation is actually trying to achieve. You must identify and verify the identity, as appropriate, of anyone who actually has influence over the management of the arrangement or its assets. You must also identify and take reasonable steps to verify all persons who actually receive benefit from it. For example a revocation of a revocable trust (partial or full) should be considered a distribution and any person receiving the proceeds (be they a beneficiary, settlor or third party) should be identified and reasonable steps should be taken on, a risk based approach, to verify the recipient. Another example includes where a person is the recipient of a loan or another benefit (e.g. tenancy of a property owned by the trust, foundation or company at lower than market rates) from a trust (or a corporate structure) then the recipient should be identified and again reasonable steps should be taken on a risk based approach to verify their identity

7. Record Keeping

All copies of customer due diligence information and transactional information must be kept for a minimum period of 6 years from the date of the transaction or the end of an ongoing business relationship.

8. Training

Section 17 of the FTRA requires reporting institutions to take all appropriate steps to ensure all of their employees and officers are regularly and appropriately trained on the risks of financial misconduct and the reporting institution's compliance programme. In regards to trustee companies it is expected that such training be given to all staff and not just the Compliance Officer and Money Laundering Reporting Officer and administration staff who deal directly with customers. As part of its responsibility to ensure that all reporting institutions are complying with all legislative requirements under the FTRA and the Regulations, the FIU will monitor and request information from trustee companies on the training programmes you undertake for staff.

9. What must be reported to the FIU?

Suspicious Activity

Any activity or requests by a client or intending client that appears to you to be unusual or suspicious in your experience with dealing with that client in particular or with clients generally must be reported to the FIU under section 47. The list in Part 5 above provides guidance as to the type and nature of transactions, events and circumstances that might give you reasonable cause to suspect an activity is suspicious.

Cash Transactions

The payment by a customer to a trustee company of an amount equal to or greater than $10,000 NZD in cash must be reported to the FIU.

10. FIU's Approach to Compliance Monitoring & Enforcement

The FIU has a responsibility to ensure that all reporting institutions are complying with all legislative requirements under the FTRA. To do this, the FIU is empowered under the Financial Intelligence Act 2015 (FIU Act) to examine your compliance with the FTRA and the Regulations. The FIU may request information from you, conduct on-site examinations and provide reports to you for this purpose.

The FIU is empowered under section 31 of the FIU Act to enforce compliance on reporting institutions that have failed to comply in whole or in part with any of the obligations under the FTRA, or have failed to undertake directives issued by the FIU to take remedial actions.

11. Penalties for Non-Compliance

Failure to comply without reasonable excuse may cause the FIU to bring legal proceedings including prosecution of which a penalty of up to $250,000 or a term of imprisonment of up to 5 years may be applied to an individual, or penalty of up to $1,000,000 for a body corporate.

12. FIU Contact

For further information about your obligations under the FTRA and Regulations, or the FIU and its activities, contact the FIU on (682) 29182 or email: intel@cifiu.gov.ck

13. Other resources

- 2008 FATF Guidance on the Risk-Based Approach for Trust and Company Service Providers (TCSPs)

http://www.fatf-gafi.org/media/fatf/documents/reports/RBA%20for%20TCSPs.pdf

- The Misuse of Corporate Vehicles, Including Trust and Company Service Providers, Feb 2007.

http://www.fatf-gafi.org/media/fatf/documents/reports/Misuse%20of%20Corporate%20Vehicles%20including%20Trusts%20and%20Company%20Services%20Providers.pdf