Targeted Financial Sanctions

Practical Guidance

Guideline No. 2 – 2015

August 2015

TARGETED FINANCIAL SANCTIONS - PRACTICAL GUIDANCE

Introduction

This guideline is for Financial Institutions (FIs) and Designated Non-Financial Businesses or Professions (DNFBPs) referred to hereinafter collectively as "Reporting Entities".

The aim of this guideline is to provide guidance to Reporting Entities that may be holding targeted funds or other assets, in preparing policies and procedures to address their legal obligations in relation to Targeted Financial Sanctions under the Anti-Money Laundering and Countering the Financing of Terrorism (AMLCFT) Act 2009, the AMLCFT (Amendment) Act 2015, the AMLCFT Regulations 2010 and other subsidiary legislation.

The information in this guideline is intended to provide general policy direction only, and does not replace the AMLCFT Act, Regulations or other subsidiary legislation.

In general terms, local **Targeted Financial Sanctions**[1] measures apply to all natural and legal persons located in Guyana or operating in or from within Guyana.

Recommendation 6 of the FATF International Standards on combating money laundering and the financing of terrorism and proliferation require countries to implement targeted financial sanctions to comply with the United Nations Security Council Resolutions (UNSCRs) that require countries to freeze, without delay, the funds or other assets of a designated person or entity, and to ensure that no funds and other assets are made available to or for the benefit of:

(i) Any person or entity designated by the UNSCR as required by Security Council resolution 1267 (1999); or

(ii) Any person or entity designated by a country pursuant to Security Council resolution 1373(2001)

Sections 2(2) and 68 of the AMLCFT Act 2009, section 18 of the AMLCFT (Amendment) Act 2015 as well as the AMLCFT Regulations 2015 stipulate provisions which address the above requirements.

Overview

Reporting Entities should aim to have proportionate systems and controls in place to reduce the risk of a targeted financial sanctions breach occurring. How those systems and controls are formulated will depend on the business model, profile and customer base of each Reporting

[1] The term *Targeted Financial Sanctions* mean both asset freezing and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of designated person or entity.

Entity. Reporting Entities should focus their resources and systems and controls on assessing where and how their particular business is most likely to breach the legal provisions related to targeted financial sanctions.
In order to assist Reporting Entities in achieving proportionate systems and controls, this guidance is divided into the following areas:

1. Implementing policies and procedures regarding Targeted Financial Sanctions.
2. Providing staff training on the implementation of Targeted Financial Sanctions measures.
3. Risk assessing Targeted Financial Sanctions vulnerabilities.
4. How to screen customers to prevent Targeted Financial Sanctions breaches.
5. How to make customer screening more effective.
6. Systems for investigating a match.
7. Action required on discovering a confirmed or potential target match.
8. International Obligations.

1. IMPLEMENTING POLICIES AND PROCEDURES REGARDING SANCTIONS

1.1 Reporting Entities should have written policies and procedures in place to deal with Targeted Financial Sanctions screening. Regular reviews and updates of Targeted Financial Sanctions policies and procedures should take place to ensure they remain fit for purpose and are enforced. The information in the following sections is an outline of areas that should be taken into account when formulating Targeted Financial Sanctions policies and procedures.

2. PROVIDING STAFF TRAINING IN SANCTIONS MATTERS

2.1 Staff should be trained on an ongoing basis with respect to the implementation of Targeted Financial Sanctions measures. As the Targeted Financial Sanctions arena is constantly evolving it is important for staff knowledge to be kept current. Training can be carried out separately or alongside anti-money laundering training so long as it is:

(i) Appropriate, accessible and routinely provided; and
(ii) Targeted to specific roles.

Detailed training may be given to those involved in customer service and monitoring, with more general training to other members of staff.

3. RISK ASSESSING TARGETED FINANCIAL SANCTIONS VULNERABILITIES

3.1 Breaching Targeted financial sanctions provisions is an absolute offence under section 18 of the AMLCFT (Amendment) Act 2015, hence the decision to take a risk-based approach is in itself a risk-based decision. If formulated properly, however, it is appropriate to take a risk-based approach to Targeted Financial Sanctions screening. If a risk-based

approach is taken, a Reporting Entity should be satisfied that its approach is appropriate and sufficient. With that in mind, it would be wise for a Reporting Entity to have a formally documented risk assessment covering Targeted Financial Sanctions measures with a clear rationale for the approach taken.

3.2 In order to conduct a comprehensive risk assessment, a business needs to have a good understanding of the Targeted Financial Sanctions regime and the risks posed by particular customers, transactions, services, products and jurisdictions.

3.3 A proper risk assessment should consider how a Reporting Entity may become involved in breaching Targeted Financial Sanctions provisions. Relevant factors a Reporting Entity may take into account in formulating its risk assessment are:

- customer, product and activity profiles;
- distribution channels;
- complexity and volume of transactions (recognising that one prohibited transaction alone would be a breach);
- processes and systems;
- operating environment;
- screening processes of intermediaries;
- geographic risk of where it does business; and
- whether trustees, settlors, beneficiaries, directors and beneficial owners of legal persons and third party payees are screened to ascertain whether there is a risk of indirect benefit to a sanctioned person.

3.4 Where, as part of a risk assessment, a Reporting Entity identifies a particular vulnerability the Reporting Entity should consider looking to ascertain the following information in order to better identify sanctions targets:

- **For individuals**: place of residence, country of birth, country of origin, citizenship, source of wealth, occupation and countries to or from which transactions are made, known associates.

- **For entities**: location of business, country in which incorporated, nature of business, beneficial owners of the business, directors, countries from which transactions are made and entities with which transactions are effected.

4. HOW TO SCREEN CUSTOMERS TO PREVENT TARGETED FINANCIAL SANCTIONS BREACHES

4.1 When screening customers Reporting Entities should attach significance to:

- Screening new customers at the commencement of a business relationship against personal identifying information on the UN Sanctions List. The UN Sanctions List can be accessed here: http://www.fiuguyana.org;

- Periodically screening existing customers, within a reasonable time of notified changes to the UN Sanctions List;
- Screening for full name, date of birth, address and aliases;
- Screening existing customers when data changes e.g. change of director;
- Ensuring payments are not indirectly made to, or for the benefit of, a designated person or entity. Thus screening of directors, beneficial owners, trustees, settlors, beneficiaries and third party payees against the UN Sanctions List is important; and
- Maintaining an audit trail of screening.

4.2 Designated persons or entities are known to use false personal information to try and evade detection. In addition, information held by an institution may not exactly correlate to information recorded on the UN Sanctions List.

4.3 The table below gives examples of how the wording or format of a customer name held by a Reporting Entity may be different from the wording used in the UN Sanctions List.

Version in the Consolidated List	**Version used by a Reporting Entity**
Revolutionary People's Liberation Army	Revolutionary Peoples' Liberation army/front
Pavlichenko, Dmitry Valeriyevich	Pavliuchenko, Dmitry Valeriyevich
Rockmans, Limited	Rockman Ltd
Salim, Ahmed Fuad	Amed Fuad Salim

4.4 To maximise screening, seek to incorporate variables such as:

- Different spellings of names (e.g. Abdul instead of Abdel);
- Name reversal (first/middle names written as surnames and vice versa);
- Shortened names (e.g. Bill instead of William);
- Maiden names;
- Removing numbers from entities; and
- Insertion/removal of full stops and spaces.

5. HOW TO MAKE CUSTOMER SCREENING MORE EFFECTIVE

5.1 To ensure customer screening is more effective, Reporting Entities should attach importance to:

- Implementing a written screening policy to incorporate the frequency of screening and quality of screening.

- Ensuring that effective sanctions screening has taken place by an intermediary, if relying on an intermediary to carry out screening. Depending on when sanctions screening took place by an intermediary, it may be necessary to re-screen to ensure the position has not changed or obtain reassurance that an intermediary's screening for sanctions is ongoing.

- Keeping customer information up to date. Complete and current customer information will improve the effectiveness of screening and reduce the amount of false positives.

Automated screening

5.2 If using automated screening, the following actions may assist to improve screening quality:

- Understanding the capabilities and limits of the particular automated screening system.
- Ensuring the system is calibrated to the institution's needs.
- Checking the matching criteria is relevant and appropriate for the nature and the size of business to ensure less false positives are produced.
- Ensuring screening rules are appropriately defined e.g. allow for the use of alternative identifiers.
- The calibration of systems to include the use of fuzzy matching. Fuzzy matching searches for words or names likely to be relevant, even if words or spelling do not match exactly. It can assist to identify possible matches where data is misspelled, incomplete or missing.
- Ensuring prominent flagging of matches so that they are clearly identifiable.
- Keeping calibration and automated systems under regular review to ensure they are fit for purpose.

6. SYSTEMS FOR INVESTIGATING A MATCH

6.1 A Reporting Entity should implement internal procedures for investigating whether a match against the UN Sanctions List is an actual match or a false positive.

6.2 In formulating such policies a Reporting Entity should consider incorporating the following actions:

- Staff should be able to seek sufficient information to enable them to confirm or eliminate a match.
- If necessary, staff should be able to make further enquiries of an intermediary, counter-party bank or the customer, or all of the above.
- Staff should be required to notify senior management of potential target

matches, particularly in cases where it cannot be determined if a potential target match is an actual target match.
- A process by which the Director, FIU is notified of confirmed matches or potential target matches that cannot be confirmed after investigation and escalation.
- Provisions for a clear audit trail of potential target matches and decisions/actions taken.

7. ACTION REQUIRED ON DISCOVERING A CONFIRMED OR POTENTIAL TARGET MATCH

7.1 In the case of a confirmed match, the Reporting Entity should:

- Comply with the freezing provision at section 18 of the AMLCFT (Amendment) Act 2015;
- Report the match to the Director, FIU. The report should include:
  - Any information held about the designated person or entity by which the person or entity can be identified.
  - The nature and amount or quantity of any funds or economic resources held by, or for, the designated person or entity.
  - Information or other matters on which the knowledge or belief reported is based.
- Comply with the Director's instructions pertaining to further dealings with the designated person or entity.

Holding an account for a designated person or entity, or processing a transaction involving a designated person or entity is not in itself grounds for filing a Suspicious Transaction Report (**"STR"**) with the FIU.

A Reporting Entity should only file a STR in relation to a designated person or entity, **if** there is a particular suspicion of criminal activity beyond the fact that the person or entity in question has been designated:

(i) by the UNSCR as required by Security Council resolution 1267; or
(ii) by the Minister responsible for Finance pursuant to Security Council resolution 1373.

8. INTERNATIONAL OBLIGATIONS

8.1 As each country's Targeted Financial Sanctions measures tend to be applicable to nationals/citizens of that country and bodies constituted or incorporated under the law of that country, wherever those persons are situated, it is important to understand any obligations that follow from having links to another country. If a Reporting Entity operates or is incorporated or constituted outside of Guyana, it should give consideration to Targeted Financial Sanctions obligations that may arise as a result. For example if you are a Guyana incorporated company

with a branch in another country, the branch in the other country should have regard to Guyana sanctions (see below). If you are a Guyanese citizen employed in an institution in another country, again Guyana sanctions should be considered.

8.2 Depending on the provider, automated screening software used in respect of customer due diligence may also provide you with international sanctions information. To give an example, "World-Check" searches in relation to a customer should highlight any sanctions measures in place internationally in respect of a person or entity.

8.3 The country profiles on websites such as www.knowyourcountry.com can also provide information on whether United Nations sanctions are in place in respect of a particular country.

APPENDIX: EXAMPLES OF GOOD AND BAD PRACTICE

Good Practice	Bad Practice
Screening of directors, beneficial owners and third party payees of corporate customers	Assuming AML customer due diligence checks include sanctions screening
Use of 'fuzzy matching' in automated screening	Failure to understand and tailor a commercially available screening system
Screening entire customer base within a reasonable time following updates to the UN Sanction List.	Screening retrospectively
Regular review of the effectiveness of policy, procedures, systems and controls	Changes to policies, procedures, systems and controls not communicated to staff
Senior management involvement when name match cannot be verified	No or insufficient senior management oversight
Clear audit trail of potential matches, decision and actions with clear rationale	Reliance on firms, consultants or intermediaries to screen without ensuring this is done effectively