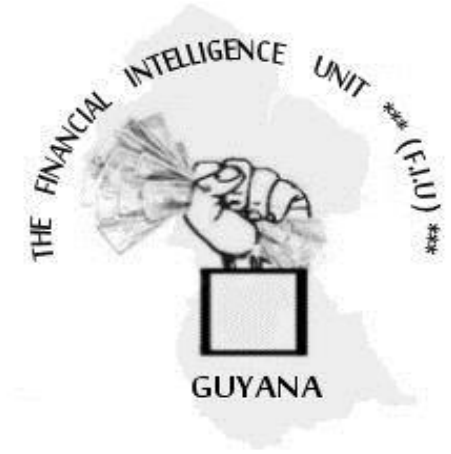
GUIDELINE NO. 1 OF 2018



DETECTING OR PREVENTING TERRORIST FINANCING

Guideline issued by the Financial Intelligence Unit
Under Section 9(4)(e)(iv) of the AMLCFT Act #13 of 2009

Published

July 2018

CONTENTS

ACRONYMS

AML/CFT	Anti-Money Laundering and Countering the Financing of Terrorism
BNI	Bearer Negotiable Instruments
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
FTF	Foreign Terrorist Fighter
NPO	Non-Profit Organisation
RE	Reporting Entity
TF	Terrorist Financing

DEFINITIONS

"Bearer negotiable instruments"

Bearer negotiable instruments include monetary instruments in bearer form such as: traveller's cheques; negotiable instruments (Including cheques, promissory notes and money orders) that are either in bearer form, endorsed without restriction, made out to a fictitious payee, or otherwise in such form that title thereto passes upon delivery; incomplete instruments (including cheques, promissory notes and money orders) signed, but with the payee's name omitted.

"Cash couriers"

The term *"cash couriers"* refer to the natural persons who physically transport currency and bearer negotiable instruments on their person or accompanying luggage from one jurisdiction to another.

Designated or specified person or entity

The term "*designated person or entity"* refers to:

(i) individuals, groups, undertakings and entities designated by the Committee of the Security Council established pursuant to resolution 1267 (1999) (the 1267 Committee), as being individuals associated with Al-Qaida, or entities and other groups and undertakings associated with Al-Qaida;

(ii) individuals, groups, undertakings and entities designated by the Committee of the Security Council established pursuant to resolution 1988 (2011) (the 1988 Committee), as being associated with the Taliban in constituting a threat to the peace, stability and security of Afghanistan, or entities and other groups and undertakings associated with the Taliban;

(iii) any natural or legal person or entity designated by jurisdictions or a supra-national jurisdiction pursuant to Security Council resolution 1373 (2001);

(iv) any natural or legal person or entity designated for the application of targeted financial sanctions pursuant to Security Council resolution 1718 (2006) and its successor resolutions by the Security Council in annexes to the relevant resolutions, or by the *"Security Council Committee established pursuant to resolution 1718 (2006)"* (the 1718 Sanctions Committee) pursuant to Security Council resolution 1718 (2006); and

(v) any natural or legal person or entity designated for the application of targeted financial sanctions pursuant to Security Council resolution 1737 (2006) and its successor resolutions by the Security Council in annexes to the relevant resolutions, or by the

"Security Council Committee established pursuant to paragraph 18 of resolution 1737 (2006)" (the 1737 Sanctions Committee) pursuant to resolution 1737 (2006) and its successor resolutions.

"Financial Institution" means any company or business that engages in any of the following activities-

(a) acceptance of deposits and other repayable funds from the public, including, but not limited to, private banking;

(b) lending, including, but not limited to, consumer credit, mortgage credit, factoring (with or without recourse), and financing of commercial transactions, including forfaiting;

(c) financial leasing other than with respect to arrangements relating to consumer products;

(d) the transfer of money or value;

(e) issuing and managing means of payment, including, but not limited to, credit cards, travellers' cheques, money orders and bankers' drafts, and electronic money;

(f) issuing financial guarantees and commitments;

(g) trading in-

(i) money market instruments, including, but not limited to, cheques, bills, certificates of deposit and derivatives;
(ii) foreign exchange;
(iii) exchange, interest rate and index instruments;
(iv) transferable securities; and
(v) commodity futures trading;

(h) participating in and underwriting securities issues and the provision of financial services related to such issues;

(i) individual and collective portfolio management;

(j) safekeeping and administration of cash or liquid securities on behalf of other persons;

(k) investing, administering or managing funds or money on behalf of other persons;

(l) underwriting and placement of life insurance and other investment-related insurance, as well as insurance intermediation by agents and brokers;

(m) money and currency changing; and

(n) such other activity, business or operation as may be prescribed by the Minister responsible for Finance[1].

"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 persons or entities[2].

"*Terrorist*" means any natural person who-

(a) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and willfully;

(b) participates as an accomplice in terrorist acts;

(c) organizes or directs others to commit terrorist acts; or

(d) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.

"*Terrorist act*" shall have the same meaning assigned to it as in the Criminal Law (Offences) Act and includes-

(a) any act which constitutes an offence within the scope of, and as defined in any of the following treaties-

I. the Convention for the Suppression of Unlawful Seizure or Aircraft (1970);

II. the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1971);

III. the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1971);

IV. the Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents (1973);

V. the International Convention against the Taking of Hostages (1979);

VI. the Convention on the Physical Protection of Nuclear Material (1980);

[1] First Schedule, AMLCFT Act 2009

[2] General Glossary FATF International Standards on Combating Money Laundering the Financing of Terrorism & Proliferation.

VII. the Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1988);

VIII. the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (1988); and

IX. the International Convention for the Suppression of Terrorist Bombings (1997); and

(b) any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation or armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a Government or an international organization to do or to abstain from doing any act.

"Terrorist financier"

A terrorist financier is any individual or legal entity that knowingly provides financial support to a terrorist, a terrorist group or terrorist organisations.

"*Terrorist financing*" means willfully providing or collecting funds, by any means, directly or indirectly, with the unlawful intention that they should be used or in the knowledge that they are to be used in full or in part-

(a) to carry out terrorist acts;

(b) by a terrorist organization; or

(c) by an individual terrorist.

"*Terrorist organization*" means any group of terrorists that –

(a) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and willfully;

(b) participates as an accomplice in terrorist acts;

(c) organizes or directs others to commit terrorist acts; or

(d) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made internationally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.

"Reporting Entity" means any person whose regular occupation or business is the carrying on of —

(a) any activity listed in the First Schedule **of** the AML/CFT Act **2009;** or

(b) any other activity defined by the Minister responsible **for** Finance as such by an order published **in** the *Gazette* amending the First Schedule[3].

"Supervisory authorities" refer to the designated competent authorities with responsibilities aimed at ensuring compliance by reporting entities with requirements to combat money laundering and terrorist financing.

TARGET AUDIENCE

The target audience of this document includes ALL reporting entities (Financial Institutions and Designated Non-Financial Businesses or Professions).

This document may also be useful to Supervisory Authorities and other competent authorities that also have the responsibility of implementing measures to combat the financing of terrorism in accordance with the requirements of the AML/CFT Act, Regulations and Guidelines and the FATF's Standards.

INTRODUCTION

When terrorists or terrorist organisations obtain their financial support from legal sources (donations, sales of publications, etc.), there are certain factors that make it more difficult to detect and trace these funds. The apparent legal sources of funding may mean that there are few, if any, indicators that would make an individual financial transaction or series of transactions stand out as linked to terrorist activities.

This document is therefore intended to enable reporting entities to protect themselves from being used as a conduit for hiding or moving terrorist funds or other assets and to ensure that they do not unwittingly hide or move terrorist funds or other assets; and to help build

[3] Section 2(1) AML/CFT Act 2009

awareness of how terrorists, their associates or those who support terrorism may use the financial system.

This document does not constitute additional rules or regulations for reporting entities. Rather, it represents guidance from the Financial Intelligence Unit as to factors associated with financial transactions that should trigger further questions on the part of the reporting entities and other competent authorities. The contents of this document are intended to clarify, complement and / or reinforce already existing due diligence requirements, along with the current policies and procedures that reporting entities are required to have in place. It should be read in conjunction with the FIU's Guidelines Nos 2 and 3 of 2015, Targeted Financial Sanctions- Practical Guidance and Targeted Financial Sanctions related to Terrorism and Terrorist Financing and the AML/CFT Act and Regulations respectively.

All reporting entities are encouraged to consider the factors outlined in this document along with policies, practices and procedures already in place for ensuring compliance with the AML/CFT Act and Regulations and for minimizing reputational risks. It should be noted as well that, while the characteristics indicated in this document may apply specifically to terrorist financing, most of them also apply in identifying suspicious transactions generally.

Reporting entities should therefore have policies and procedures that will assist in the detection and deterrence of transactions that may involve funds used in terrorist financing. The increased scrutiny that may be warranted for some transactions should be seen as a further application of the institution's due diligence and anti-money laundering policies and procedures and should lead, when appropriate, to reporting of such financial activity to the FIU as suspicious transactions in accordance with section 18(4) of the AML/CFT Act.

To ensure that the practical steps are taken to increase scrutiny of certain transactions when necessary, reporting entities should review their practices in relation to the detection and reporting of transactions relating to terrorist financing, as part of their general internal and external audit processes. Reporting entities should implement measures or procedures to mitigate risks based on the products and services offered, and the nature, size and complexity of their business.

This document should not be interpreted as discouraging or prohibiting reporting entities from doing business with any legitimate customer. It is designed solely as a means of assisting reporting entities in determining whether a transaction merits additional scrutiny so that the institution is better able to identify, report (when appropriate) and ultimately avoid transactions involving funds supporting or associated with the financing of terrorism.

CHARACTERISTICS OF TERRORIST FINANCING

Terrorists often control funds from a variety of sources around the world and employ increasingly sophisticated techniques to move these funds between jurisdictions. In doing so, they draw on the services of professionals such as bankers, accountants and lawyers, and take advantage of a range of financial services products, new technologies (social media) and payment methods.

While the total funds required by terrorist networks may be large, the funding required to finance individual terrorist attacks may be small. For example, according to the FATF's Guidance for Financial Institutions in detecting terrorist financing, published on April 24, 2002, experts that examined the financial connections among the September 11th hijackers reported that most of the individual transactions were small sums, that is, below the usual cash transaction reporting thresholds, and in most cases the operations consisted of only wire transfers. The individuals were apparently foreign students who appeared to be receiving money from their parents or in the form of grants for their studies, thus the transactions would not have been identified as needing additional scrutiny by the financial institutions involved.

SOURCES OR TERRORIST FINANCING

According to the FATF Guidance for FIs in Detecting Terrorist Financing 2002, terrorist financing comes from the following two primary sources:

I. **State Sponsored Terrorism** - Financial support provided by States or organisations with large enough infrastructures to collect and then make funds available to the terrorists; or

II. **Self-Sponsored Terrorism** - Legitimate or illegitimate revenue-generating activity committed by terrorist organisations themselves.

As with criminal organisations, a terrorist group's income may be derived from crime or other unlawful activities. The Commonwealth Secretariat[4] highlighted the following financing activities as typical:

- ***Extortion and Kidnapping***

  This form of fundraising continues to be one of the most prolific and highly profitable. Monies are usually raised from within communities of which terrorists are an integral part in return for 'protection', usually against the terrorist themselves. Over time, extortion comes to be regarded as a cost of doing business in communities where it is prevalent, and payments for individuals or businesses become essential to obtain the release of kidnapped family members, colleagues or employees. A terrorist group in a particular region may support itself through these criminal activities.

- ***Smuggling***

  Smuggling across borders has become one of the most profitable activities for terrorist organisations. Successful smuggling operations require co-ordination and established distribution networks through which smuggled goods can be sold for profit. The illegal smuggling profits are 'placed' into the banking system with the use of front companies or shell companies that are dissolved after they have fulfilled their purpose. Alternatively, legitimate 'front' businesses may be used to pay in the smuggled funds as part of their normal turnover. In some cases, businesses extorted by terrorist organisations are coerced in placing criminal proceeds.

- ***Drug Trafficking***

  The proceeds of drug trafficking activity can be a highly profitable source of funds for terrorist groups and nation states that sponsor terrorism. Even if a terrorist group is not directly involved in the importation or distribution of drugs, they often profit from the activity by allowing drug suppliers and dealers to operate within the communities that they control, and through the imposition of levies.

[4] Combating Money Laundering and Terrorist Financing, A Model of Best Practice for the Financial Sector, the Professions and Other Designated Businesses – Second Edition

- ***Charities and Fundraising***

  Knowingly or not, charitable organizations have served as vehicles for raising and laundering funds destined for terrorism. In many cases, the charities to which donations are given are in fact legitimate in that they do engage in some of the work they purport to carry out.

Reporting entities, particularly financial institutions, should take note that charities or non-profit organizations have the following characteristics that are particularly vulnerable to misuse for terrorist financing:

- Enjoying the public trust.
- Having access to considerable sources of funds.
- Being cash-intensive.
- Frequently having a global presence, often in or next to areas exposed to terrorist activity.
- Often being subject to little or no regulation and/or having few obstacles to their creation.

- ***Donations***

  It is common practice within certain ethnic communities for amounts calculated as a percentage of income to be donated automatically to charity. It would be wrong to assume that such donations are either made with the intention of being of benefit to terrorist or they are used for this purpose. Nevertheless, it must be recognized that both community donations and donations from wealthy private individuals and nation states that support terrorism are an import source of funding for many terrorist organisations.

EMERGING RISKS FOR TERRORIST FINANCING

According to the FATF's 2015 Report on Emerging Terrorist Financing Risks, rising threats and vulnerabilities include:

I. *Self-funding by foreign terrorist fighters (FTFs)*

The advent of social media, smartphone applications, and internet sharing sites now provide terrorist organizations global reach at little to no cost. Foreign terrorist fighters (FTFs) and terrorist

sympathizers can self-radicalize and/or communicate with terrorist organizations like never before. The low cost associated with perpetrating a terrorist act on a "soft target" (i.e., a civilian, non-military target that is relatively unprotected and thus vulnerable to terrorist attacks) means such acts can be self-funded. Self-funding includes sources such as employment income, social assistance, family support, and bank loans, which makes detection early impossible without the association of other aggravating terrorist financing indicators.

II. *Raising Funds through the use of Social Media*

Social media has created the ability to build social and information-sharing networks like never before in human history. This incredible advance in technology presents a unique opportunity for terrorist organizations to communicate and raise money for their causes, and the potential to reach into every home in every country in near real time. Crowdfunding and sharing of virtual or prepaid account information are a few of the methods through which social media has been leveraged by terrorists. This presents unique difficulties for law enforcement not only due to the increased dispersion of the activity but also the need for cooperation from both financial institutions and social media platforms.

III. *New Payment Products and Services*

The internet, new payment platforms, and electronic money have changed the way people conduct business, transact with each other, and how consumers buy products and services. Whereas a small corner shop was limited to servicing local consumers, it can now have a broader, global reach with an online business as well. Digital payment platforms have altered how a consumer and the regulatory environment view a merchant or funds transmission. The cheaper cost of technology and our globally interdependent society, increasingly highly skilled engineering-based workforce, and entrepreneurial drive have all contributed to the evolution of new payment products and services pushing the boundaries of how and where money is used. Generally, the risk posed by these new payment systems is relative to the functionality of the service and their funding mechanisms.

IV. *Exploitation of Natural Resources*

Terrorist organizations that hold or maintain control over territory or operate in a country with poor governmental control of the territory may take control of natural resources such as gas, oil, timber, diamonds, gold (and other precious metals), wildlife (e.g., ivory trading), and historical artifacts, or extort companies that extract those resources to both fund terrorist acts and support day-to-day activities. These resources themselves may be sold on the black market or to complicit companies where they can then be integrated into the global trade sector. An awareness of geographies where terrorist organizations operate or maintain control, current commodity prices, and strong multi-jurisdictional partnerships are necessary to combat this method of terrorist funding which has the potential to generate vast sums.

LAUNDERING OF TERRORIST-RELATED FUNDS

From a technical perspective, the methods used by terrorists and their associates to generate funds from illegal sources differ little from those used by traditional criminal organisations. One would tend to believe that there is no need to launder funds acquired from legitimate sources. However, a terrorist group needs to disguise links between their illegitimate and legitimate funding sources, in order to use them without attracting the attention of the competent authorities.

Below are some of the particular methods detected by FATF with respect to various terrorist groups:

i. cash smuggling (both by couriers or bulk cash shipments),
ii. structured deposits to or withdrawals from bank accounts,
iii. purchases of various types of monetary instruments (travellers' cheques, bank cheques, money orders),
iv. use of credit or debit cards, and
v. wire transfers.

There have also been indications that some forms of underground banking (particularly the *hawala* schemes) have had a role in moving terrorist related funds.

The difference between legally and illegally obtained proceeds raises an important legal problem as far as applying AML measures to terrorist financing. Money laundering has generally been defined as a process whereby funds obtained through or generated by criminal activity are moved or concealed in order to obscure the link between the crime and generated funds. The terrorist's ultimate aim on the other hand is not to generate profit from his fundraising mechanisms but rather to obtain resources to support his operations.

PROTECTING VULNERABLE SECTORS

Guyana has an obligation to protect its financial and other sectors from money laundering and the financing of terrorism, and in this regard is guided by the FATF Recommendations, and the relevant legislation which have further reduced the requirements of FATF into law.

- ***Formal Financial Sector***

With respect to the financial sector, FATF Recommendation 16 was developed with the objective of preventing terrorists and other criminals from having unchallenged access to wire transfers for moving their funds, and for detecting such misuse when it occurs. Specifically, it aims to ensure that basic information on the originator and beneficiary of wire transfers is immediately available to:

(I) appropriate law enforcement and/or prosecutorial authorities to assist them in detecting, investigating, prosecuting terrorists or other criminals and tracing the assets of terrorists or other criminals;

(II) financial intelligence units for analysing suspicious or unusual activity, and disseminating it as necessary; and

(III) to ordering, intermediary and beneficiary financial institutions to facilitate the identification and reporting of suspicious transactions, and to implement the requirements to take freezing action and comply with prohibitions from conducting transactions with designated persons and entities.

In keeping with the objectives of the Recommendation 16, Guyana included relevant provisions in the AML/CFT (Amendment) Acts and AML/CFT Regulations of 2015.

- ***Charitable Sector***

With respect to charitable organisations, FATF Recommendation 8, lays out a framework that aims to protect the non-profit organization (NPO) / charitable sector by ensuring it is not misused by terrorist organisations that:

(a) pose as legitimate entities;
(b) exploit legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset freezing measures; or
(c) conceal or obscure the clandestine diversion of funds intended for legitimate purposes but are diverted for terrorist purposes.

Toward this aim, FATF has developed an effective four-prong approach to identifying, preventing and combating terrorist misuse of charities that focuses on:

(1) outreach to the charitable sector;
(2) supervision or monitoring of the sector;
(3) information gathering and investigation of terrorists and their networks that abuse the charitable sector; and
(4) international engagement to protect the sector globally.

It is therefore very important that the supervisory authority for Charities/Non-Profit Organizations be vigilant in its efforts to ensure that these reporting entities are:

1. Properly licensed or registered;
2. Maintaining information on the purpose and objectives of their stated activities; and the identify of controlling bodies such as senior officer, board members and trustees;
3. Issuing annual financial statements;
4. Putting appropriate controls in place to ensure that all funds are fully accounted for, and are spent in a manner that is consistent with the purpose and objectives of the entity's stated activities;

5. Taking reasonable measures to confirm the identity, credentials and good standing of beneficiaries and associate NPOs; and
6. Maintaining records of domestic and international transactions.

- ***Cash Couriers***

With respect to cash couriers, FATF Recommendation 32, was developed with the objective of ensuring that terrorists and other criminals cannot finance their activities or launder the proceeds of their crimes through physical cross-border transportation of currency and bearer negotiable instruments (BNIs). Specifically, it aims to ensure that countries have measures to:

(1) detect the physical cross-border transportation of currency and BNIs;
(2) stop or restrain currency and bearer negotiable instruments that are suspected to be related to terrorist financing or money laundering;
(3) stop or restrain currency or BNIs that are falsely declared or disclosed;
(4) apply appropriate sanctions for making a false declaration or disclosure; and
(5) to enable confiscation of currency or BNIs that are related to terrorist financing or money laundering.

The Guyana Revenue Authority which is responsible for monitoring cross border transportation of currency and BNIs in Guyana, is therefore encouraged to ensure that travellers are aware of their obligation to declare foreign currency amounting to more than ten thousand United States dollars or its equivalent in any other currency. Although every citizen/resident is assumed to be responsible for knowing and complying with the law, it is a best practice for jurisdictions to make the declaration requirements explicitly and clearly known to all travellers, especially at ports of entry and border crossings. This will enhance the overall effectiveness of the system, including the ability to successfully prosecute persons for "failure to declare" or "false declarations".

RECOGNISING TERRORIST FINANCING

Some important aspects of terrorist financing that make its detection more difficult are the size and nature of the transactions involved. Several FATF experts have mentioned that the funding

needed to mount a terrorist attack does not always call for large sums of money, and the associated transactions are usually not complex.

Indeed, the only time that reporting entities might clearly identify terrorist financing as distinct from other criminal misuse of the financial system is when a known terrorist or terrorist organisation attempts to open an account. Reporting entities are, however, in a position to detect suspicious transactions that, if reported, may later prove to be related to terrorist financing. It is the duty of the FIU to analyse all reported suspicions to determine whether the transactions relate to a particular type of criminal or terrorist activity and decide on a course of action. For this reason, reporting entities may seek to determine the legality of the source or destination of the funds. They should also establish whether transactions are unusual, suspicious or otherwise indicative of any criminal or terrorist activity.

SANCTIONS

- ***Terrorist financiers***

The financing of terrorism is an indictable offence under section 68 of the AML/CFT Act. Penalties include,

a) Seizure and detention of terrorist cash, to cut off cash flows to individual terrorists and terrorist organisations.
b) Fines – if act resulted in the death of any person – a fine of not less than one million five hundred thousand dollars together with death.
   In any other case – a fine of not less than five hundred thousand dollars together with imprisonment for ten to fifteen years.
c) Freezing of, or prohibiting access to, funds or other assets to prevent them from being made available, directly or indirectly, for the benefit of a designated or specified person or entity.

- ***Targeted Financial Sanctions***

FATF Recommendation 6 calls on countries to develop and implement targeted financial sanctions regimes that identify, freeze the assets of, and prohibit making funds available to designated terrorists and their support networks without delay. These requirements are necessary to deprive

terrorists and terrorist networks of the means to conduct future terrorist activity and maintain their infrastructure and operations.

Again, in keeping with the requirement of the FATF Recommendations, section 68(A) of the AML/CFT Act 2009 prohibits a reporting entity from knowingly -

(a) Dealing directly or indirectly with any property of a designated or specified person or entity/ a terrorist or terrorist organization, including funds derived or generated from property owned or controlled directly or indirectly by designated or specified person or entity/ a terrorist or terrorist organization
(b) Entering into or facilitating, directly or indirectly, any transaction related to a dealing referred to above;
(c) Providing any financial or other related service in respect of the property referred to above;
(d) Making any property or any financial or other related service available, directly or indirectly for the benefit of a listed person or entity/ a terrorist or terrorist organization.

In addition, a reporting entity is required to immediately report to the Director of the FIU, if it is in possession or control of any funds or other assets of a listed/designated person or entity. *(See Guideline No. 2 of 2016 on Terrorist Property Reporting)*

A reporting entity that contravenes any of the above provisions commits an offence and shall be liable on summary conviction to a fine between five million and one hundred million or imprisonment to up to seven years where it is a natural person; and a fine between ten million to two hundred million dollars where it is a body corporate.

Reporting entities are reminded of the importance of having and/ or maintaining an effective system to screen customers so as to prevent breaches of targeted financial sanctions. New customers should be screened at the commencement of a business relationship, and existing customers periodically, within a reasonable time of updates to the UN Sanctions List or List issued by the Minister of Finance. Note that these updates are communicated to REs periodically by the REs respective supervisory authority based on notification from the FIU.

Screening involves the RE determining whether a new or existing customer is featured on the UN Sanctions List or List issued by the Minister of Finance for the purpose of implementing targeted financial sanctions in accordance with the AML/CFT Act and Regulations.

SUSPICIOUS OR UNUSUALLY FINANCIAL ACTIVITIES/TRANSACTIONS THAT MAY BE A CAUSE FOR INCREASED SCRUTINY

As a normal part of carrying out their work, reporting entities should be aware of elements of individual transactions that could indicate funds involved in terrorist financing. The following list of potentially suspicious or unusual activities is meant to show types of transactions that could be a cause for additional scrutiny. This list is not exhaustive, nor does it take the place of any legal obligations related to the reporting of suspicious transactions to the FIU.

The list of characteristics should be taken into account by reporting entities along with other available information including any lists of suspected terrorists, terrorist groups, and associated individuals and entities issued by the United Nations or the Minister of Finance, the nature of the transaction itself, and the parties involved in the transaction. The existence of one or more of the factors described in the following list may warrant some form of increased scrutiny of the transaction. However, the existence of one of these factors by itself does not necessarily mean that a transaction is suspicious or unusual.

To avoid becoming conduits for terrorist financing, reporting entities must look at, among other things, the following factors:

A. Accounts

- Accounts that receive relevant periodical deposits and are dormant at other periods. These accounts are then used in creating a legitimate appearing financial background through which additional fraudulent activities may be carried out.

- A dormant account containing a minimal sum suddenly receives a deposit or series of deposits followed by daily cash withdrawals that continue until the transferred sum has been removed.

- When opening an account, the customer refuses to provide information required by the financial institution, attempts to reduce the level of information provided to the minimum or provides information that is misleading or difficult to verify.

- An account for which several persons have signing authority, yet these persons appear to have no relation among each other (either family ties or business relationship).

- An account opened by a legal entity or an organisation that has the same address as other legal entities or organisations, but for which the same person or persons have signing authority, when there is no apparent economic or legal reason for such an arrangement (for example, individuals serving as company directors for multiple companies headquartered at the same location, etc.).

- An account opened in the name of a recently formed legal entity and in which higher than expected level of deposits are made in comparison with the income of the founders of the entity.

- The opening by the same person of multiple accounts into which numerous small deposits are made that in aggregate are not commensurate with the expected income of the customer.

- An account opened in the name of a legal entity that is involved in the activities of an association or foundation whose aims are related to the claims or demands of a terrorist organisation.

- An account opened in the name of a legal entity, a foundation or an association, which may be linked to a terrorist organisation and that shows movements of funds above the expected level of income.

B. Deposits and withdrawals

- Deposits for a business entity in combinations of monetary instruments that are atypical of the activity normally associated with such a business (for example, deposits that include a mix of business, payroll and national insurance cheques).

- Large cash withdrawals made from a business account not normally associated with cash transactions.

- Large cash deposits made to the account of an individual or legal entity when the apparent business activity of the individual or entity would normally be conducted in cheques or other payment instruments.

- Mixing of cash deposits and monetary instruments in an account in which such transactions do not appear to have any relation to the normal use of the account.

- Multiple transactions carried out on the same day at the same branch of a financial institution but with an apparent attempt to use different tellers.

- The structuring of deposits through multiple branches of the same financial institution or by groups of individuals who enter a single branch at the same time.

- The deposit or withdrawal of cash in amounts which fall consistently just below identification or reporting thresholds.

- The presentation of uncounted funds for a transaction. Upon counting, the transaction is reduced to an amount just below that which would trigger reporting or identification requirements.

- The deposit or withdrawal of multiple monetary instruments at amounts which fall consistently just below identification or reporting thresholds, particularly if the instruments are sequentially numbered.

C. Wire Transfers

- Wire transfers ordered in small amounts in an apparent effort to avoid triggering identification or reporting requirements.

- Wire transfers to or for an individual where information on the originator, or the person on whose behalf the transaction is conducted, is not provided with the wire transfer, when the inclusion of such information would be expected.

- Use of multiple personal and business accounts or the accounts of non-profit organisations or charities to collect and then funnel funds immediately or after a short time to a small number of foreign beneficiaries.

- Foreign exchange transactions that are performed on behalf of a customer by a third party followed by wire transfers of the funds to locations having no apparent business connection with the customer or to countries of specific concern.

D. Characteristics of the customer or his/her business activity

- Funds generated by a business owned by individuals of the same origin or involvement of multiple individuals of the same origin from countries of specific concern acting on behalf of similar business types.

- Shared address for individuals involved in cash transactions, particularly when the address is also a business location and/or does not seem to correspond to the stated occupation (for example student, unemployed, self-employed, etc.).

- Stated occupation of the person transacting the business is not commensurate with the level or type of activity (for example, a student or an unemployed individual who receives or sends large numbers of wire transfers, or who makes daily maximum cash withdrawals at multiple locations over a wide geographic area).

- Regarding non-profit or charitable organisations, financial transactions for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organisation and the other parties in the transaction.

- A safe deposit box is opened on behalf of a commercial entity when the business activity of the customer is unknown, or such activity does not appear to justify the use of a safe deposit box.

- Unexplained inconsistencies arising from the process of identifying or verifying the customer (for example, regarding previous or current country of residence, country of issue of the passport, countries visited according to the passport, and documents furnished to confirm name, address and date of birth).

E. Transactions linked to location of concern

- Transactions involving foreign currency exchanges that are followed within a short time by wire transfers to locations of specific concern (FATF non-cooperative countries and territories).

- Deposits are followed within a short time by wire transfers of funds, particularly to or through a location of specific concern (for example, FATF non-cooperative countries and territories).

- A business account through which a large number of incoming or outgoing wire transfers take place and for which there appears to be no logical business or other economic purpose, particularly when this activity is to, through or from locations of specific concern.

- The use of multiple accounts to collect and then funnel funds to a small number of foreign beneficiaries, both individuals and businesses, particularly when these are in locations of specific concern.

- A customer obtains a credit instrument or engages in commercial financial transactions involving movement of funds to or from locations of specific concern when there appears to be no logical business reasons for dealing with those locations.

- The opening of accounts of financial institutions from locations of specific concern.

- Sending or receiving funds by international transfers from and/or to locations of specific concern.

CONCLUSION

Detecting and tracing funds related to terrorist financing will continue to be a challenge for reporting entities as long as charities, non-profit organisations and other legal organisations continue to play such an important role in the financing of terrorist groups. Transactions related to terrorist financing are also difficult to detect as they are, in most instances, small and simple/routine. Notwithstanding, reporting entities are uniquely positioned (with the appropriate guidance and training), to detect suspicious or unusual transactions that, if reported, may later prove to be related to terrorist financing. Reporting entities are therefore urged to be vigilant to safeguard against being used as conduits for the financing of terrorism and to report all transactions indicative of criminal or terrorist activity to the FIU.

SOURCES OF INFORMATION

Several sources of information exist that may help reporting entities in determining whether a potentially suspicious or unusual transaction could indicate funds involved in the financing of terrorism and thus be subject to reporting obligations under the AML/CFT Act and Regulations. These include the following:

1. UNITED NATIONS LISTS
   Committee on S/RES/1267 (1999)
   Website: http://www.un.org/Docs/sc/committees/AfghanTemplate.htm

2. OTHER LISTS
   (i) Financial Action Task Force
   FATF Identification of Non-Cooperative Countries and Territories
   FATF Website: http://www.fatf-gafi.org/NCCT_en.htm

   (ii) United States
   Executive Order 13224, 23 September 2001 (with updates)
   US Department of the Treasury
   Website: http://www.ustreas.gov/terrorism.html

   (iii) Council of the European Union
   Council Regulation (EC) Nº 467/2001 of 6 March 2001 [on freezing Taliban funds]

   Council Decision (EC) Nº 927/2001 of 27 December 2001 [list of terrorist and terrorist organisations whose assets should be frozen in accordance with Council Regulation (EC) Nº 2580/2001]

   Council Common Position of 27 December 2001 on application of specific measures to combat terrorism [list of persons, groups and entities involved in terrorist acts]
   EUR-lex website: http://europa.eu.int/eur-lex/en/index.html

3. STANDARDS
   (i) Financial Action Task Force
   FATF Special Recommendations on Terrorist Financing
   FATF website: http://www.fatf-gafi.org/TerFinance_en.htm
   FATF Forty Recommendations on Money Laundering
   FATF website: http://www.fatf-gafi.org/40Recs_en.htm

   (ii) UN Conventions and Resolutions
   International Convention on the Suppression of Terrorist Financing
   Website: http://untreaty.un.org/English/Terrorism.asp

UN Security Council Resolutions on Terrorism
Website: http://www.un.org/terrorism/sc.htm

(iii) Council of the European Union

Council Regulation (EC) Nº 2580/2001 of 27 December 2001 on specific restrictive measures directed against certain persons and entities with a view to combating terrorism
EUR-lex website: http://europa.eu.int/eur-lex/en/index.html

REFERENCES

- Anti-Money Laundering and Countering the Financing of Terrorism Act No. 13 of 2009.
- Anti-Terrorism and Terrorist Related Activities Act No. 15 of 2015.
- Combating Money Laundering and Terrorist Financing, A Model of Best Practice for the Financial Sector, the Professions and Other Designated Businesses (Second Edition) – Commonwealth Secretariat.
- FATF (2002), Guidance for Financial Institutions in Detecting Terrorist Financing.
- FATF (2012), International Standards on combating money laundering and the financing of terrorism and proliferation.
- FATF (2013), Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems.
- FATF (2015), Emerging Terrorist Financing Risks