TURKS AND CAICOS ISLANDS
FINANCIAL SERVICES COMMISSION

TERRORIST FINANCING GUIDANCE
FOR
NON-PROFIT ORGANISATIONS, FINANCIAL INSTITUTIONS, AND DESIGNATED NON-FINANCIAL BUSINESSES & PROFESSIONS

28 March 2023

Contents

TERMINOLOGY

Customer Due Diligence (CDD)

CDD includes;

- Identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from customer or through reliable and independent source.

- Identifying, where there is a beneficial owner who is not the customer, the beneficial owner and taking adequate measures to verify his identity so that the financial business is satisfied that it knows who the beneficial owner is, including, in the case of a legal person, trust or similar legal arrangement, measures to understand the ownership and control structure of the person, trust or arrangement.

- Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship; and

- Monitoring of accounts/transactions on ongoing basis to ensure that the transactions being conducted are consistent with the financial business's knowledge of the customers, their business and risk profile, including, where necessary, the source of funds and, updating records and data/ information to take prompt action when there is material departure from usual and expected activity through regular matching with information already available with the financial business;

Designated Non-Financial Business and Profession (DNFBP)

A financial business, as set out under Schedule 2 of the Anti-Money Laundering and Prevention of Terrorist Financing Regulations 2010 (AML Regulations), that is not a regulated financial business as set out under Schedule 1 of the AML Regulations.

Financial Action Task Force (FATF)

The Financial Action Task Force (FATF) is an inter-governmental organisation that designs and promotes policies and standards to combat financial crime. Recommendations created by FATF target money laundering, terrorist financing, and other threats to the global financial system. FATF was created in 1989 at the behest of the G7 and is head-quartered in Paris.

Financial Institution (FI)

A financial business that has been issued a license under a regulatory ordinance.

Non-Profit Organisation (NPO)

An organisation that — (a) is established solely or primarily for charitable, religious, cultural, educational, social or fraternal purposes or for the purpose of benefiting the public or a section of the public; and (b) raises or disburses funds in pursuance of those purposes.

Terrorist

The term terrorist is defined by the FATF as any natural person who: (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and wilfully; (ii) participates as an accomplice in terrorist acts; (iii) organises or directs others to commit terrorist acts; or (iv) 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

The FATF defines a terrorist act as including any 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 of 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 organisation to do or to abstain from doing any act.

Terrorist financing

The term terrorist financing is defined by the FATF as the financing of terrorist acts, and of terrorists and terrorist organisations.

Terrorist organisation

As defined by the FATF, a term terrorist organisation refers to any group of terrorists that: (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and wilfully; (ii) participates as an accomplice in terrorist acts; (iii) organises or directs others to commit terrorist acts; or (iv) 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.

INTRODUCTION

The main objective of carrying out terrorist acts is to intimidate a population or compel a government to do something. This is done by intentionally killing, seriously harming, or endangering an individual or individuals, or causing substantial property damage that is likely to seriously harm people. It can also be done by seriously interfering with or disrupting essential services, facilities, or systems.

Terrorists need financial support to carry out terrorist activities and achieve their goals. In this respect, there is little difference between terrorists and other criminals in their use of the financial system. A successful terrorist group, much like a criminal organisation, is one that can build and maintain an effective financial infrastructure. For this, it must develop sources of funding and means of obscuring the links between those sources and the activities the funds support. It needs to find a way to make sure that the funds are available and can be used to obtain whatever goods or services needed to commit terrorist acts.

The fundamental aim of terrorist financing is to obtain resources to support terrorist activities. The sums needed to mount terrorist attacks are not always large and the associated transactions are not necessarily complex. While there is no known presence of terrorists or affiliation with external terrorists and terrorist organisations, international financial centres like the TCI can be exploited by terrorist financiers to enable financial flows or assist in the shipment of illicit goods, services and technology needed for supporting terrorism.

Disrupting funding flows creates a hostile environment for terrorism, constraining overall capabilities of terrorists and helping frustrate their ability to execute terrorist acts. Therefore, preventing terrorist financing is an important part of combatting terrorist financing. It is essential to prevent terrorist financing and disrupt the financial support that terrorists need.

This paper will describe what is terrorist financing and will outline the legal obligations of NPOs, FIs and DNFBPs regarding terrorist financing, the characteristics that makes certain sectors more vulnerable to TF than others, as well as indicators for TF. The paper will also outline preventative measures that FIs, NPOs and DNFBPs can take under the TCI's AML/PTF framework.

SCOPE AND OBJECTIVES OF GUIDANCE

To whom does this Guidance apply?

This guidance applies to NPOs, FIs and DNFBPs, which include the following categories of business and professions as listed in Schedule 2 of the AML Regulations:

- Banks
- Money Service Businesses
- Trust Companies

- Company Managers and Agents
- Investment Dealers
- Long Term Insurers
- Independent Legal Professions
- Accountants, Auditors and Bookkeepers
- Realtors
- Jewellers
- Pawn Shops
- Vehicle Dealers
- Boat Dealers
- Lenders
- Debt Purchasers
- Payment Service Providers

Related Guidance Documents

This guidance should be read in conjunction with the following documents:

- The Commission's Proliferation Financing Guidance;
- The Commission's DNFBP Customer Due Diligence Guidance;
- The Commission's Guidelines on Risk Assessment;
- Targeted Financial Sanctions Guidance for Financial Institutions and DNFBPs;
- Financial Sanctions Guidance issued by the Attorney General's Chambers;
- TCI Financial Sanctions Survey Report;
- Prevention of Terrorism Ordinance (PTO);
- Proceeds of Crime Ordinance (POCO);
- Anti-Money Laundering and Prevention of Terrorist Financing Regulations;
- Anti-Money Laundering and Prevention of Terrorist Financing Code;
- Anti-Money Laundering and Prevention of Terrorist Financing Guidance Notes;
- Non-Profit Organisations Registration Guideline;
- Guideline Number 1 of 2019 For Non-Profit Organisations;

- NPO Supervisory Advisory on Internal Financial Controls for NPOs; and
- NPO Help Sheet.

STATUS OF THIS GUIDANCE

This guidance is supplemental to the Prevention of Terrorism Ordinance, the Non-Profit Organisations Regulations, Anti-Money Laundering and Prevention of Terrorist Financing Regulations (AML Regulations) and Anti-Money Laundering and Prevention of Terrorist Financing Code. (AML Code). It is not legal advice and is not intended to replace the Prevention of Terrorism Ordinance, Non-Profit Organisations Regulations, AML Regulations, and the AML Code. The guidance is intended for use by controllers of NPOs and senior management and compliance staff of FIs and DNFBPs to assist in the development of internal systems and controls. Compliance with this guidance will be taken into consideration by the Commission when assessing an NPO's, FI's or DNFBP's compliance with their legal obligations.

TCI TF LEGAL FRAMEWORK

The FATF Recommendation 5 requires countries to criminalise terrorist financing. The United Kingdom, through order in council made pursuant to United Nations Security Council Resolution 1373, extended the Terrorism (United Nations Measures) (Overseas Territories) Order, 2001 to the TCI. The law created several criminal offences related to terrorism.

Article 3 (Collection of funds) criminalises the act of soliciting, receiving, or providing funds with knowledge or intent that will or may be used for the purposes of terrorism.

Article 4 (Making funds available) further extends criminal liability to making any funds or financial services available directly or indirectly for the benefit of persons committing, attempting to commit, facilitating or participating in an act of terrorism. Article 2 defines 'funds' consistent with the definition in the UN Convention on the Suppression of Financing of Terrorism.

To implement the FATF Recommendation 5, the TCI enacted the Prevention of Terrorism Ordinance 2014 which criminalises terrorism and terrorist financing, in accordance with the United Nations Convention on the Suppression of Financing of Terrorism. The Proceeds of Crime Ordinance 2007 introduced a comprehensive framework to detect and deter money laundering and terrorist financing and introduced measures to prevent the flow of illicit funds and to combat transnational crime. These laws assist in protecting the financial integrity of the TCI's financial system.

Section 10 of the PTO makes it an offence to invite another to provide property for the purposes of terrorism, to receive or provide property intending that it be used, or having reasonable cause to suspect that it may be used, for the purposes of terrorism. Section 2 of the PTO defines property as including money, goods, things in action, land, and every description of property, whether real or

personal, movable or immovable, vested or contingent, and whether situated in the Islands or elsewhere. Section 4 of the PTO defines 'terrorist property' as property which is 'likely to be used' for the purposes of terrorism and proceeds from the commission of acts of terrorism.

Section 11 of the PTO makes it an offence for a person to use property for the purposes of terrorism or to possess property intending that it be used, or having reasonable cause to suspect that it may be used, for the purposes of terrorism.

Section 12 of the PTO makes it an offence to enter into or become concerned with an arrangement which facilities the retention or control by or on behalf of another person of terrorist property by concealment, by removal from the jurisdiction or by transfer to nominees.

Section 13 of the PTO makes it an offence for a person to attempt to commit any of the offences in sections 10 to 12.

Section 4(1)(d) of the Financial Services Commission Ordinance and section 161(3)(a) of the POCO establishes the role of the Financial Services Commission to monitor compliance by NPOs, FIs and DNFBPs with their AML/PTF obligations set out in the AML/PTF Regulations and such other Ordinances, regulations, codes, or guidance relating to money laundering or the financing of terrorism. The referenced legislation requires NPOs, FIs and DNFBPs to ascertain the risk of money laundering, terrorist financing and proliferation financing that they are exposed to, to apply appropriate internal controls to manage this risk, to keep records, to vet and train staff, and to periodically assess the effectiveness of their AML/PTF Compliance Program.

NPOs, FIs and DNFBPs play a vital role in preserving the integrity of the TCI and the TCI's financial system. The identification, assessment, understanding, and management of TF risks by NPOs, FIs and DNFBPs is essential to a robust AML/PTF regime. It is critical that every NPO, FI and DNFBP includes prevention of terrorist financing (PTF) in their AML/PTF programme and risk management strategies.

ML vs TF and PF

Differences between Money Laundering, Terrorist Financing and Proliferation Financing:

	Money Laundering (ML)	Terrorist Financing (TF)	Proliferation Financing (PF)
Purpose	Use of illicit funds in the regulated system	Supports terrorist activities	Acquisition of Weapons of Mass Destruction
Source of Funds	From illegitimate activities. Funded via the illicit activity of the criminal/criminal organisation ie corruption, tax evasion, the sale of	From illegitimate/legitimate activities Numerous funding streams, including, for example:	Often state-sponsored programs but also through fundraising activities by non-state actors

	drugs, robberies, ransomware attacks, illegal arms trade, prostitution, etc. The crime may not have been committed in TCI. Organised crime groups may collaborate with terrorists and may also be classified as proscribed terrorist organisations.	– Sponsored by financier/benefactor sympathetic to the cause – Self-funded – Funds raised via commercial activities (e.g. web shops, music festivals) – Funds raised via organised fund-raising activities (e.g. via non-profit sector, social media, crowdfunding platforms, groups' own magazines) – Exploitation of natural resources in conflict zones (e.g. ISIL – Oil in the Middle East; Al-Shabaab – Gold in West Africa and Daesh – Timber in East Africa) – Looting and sale of cultural artifacts – Real estate (generating income, acting as an investment, and which certain terrorist groups use as club houses etc.) It is not unusual for terrorists to be involved in, or operating in close proximity to, conflict zones and criminal methods to raise funds tend to emerge, either in isolation or working with criminal groups (e.g. illicit smuggling, human trafficking, extortion, drugs trafficking and kidnap for ransom). The United Nations reports that during the COVID-19 pandemic cash smuggling to territories where Daesh was active became less prominent, whilst crypto transfers increased (e.g. using personal crypto wallets).	
Conduits	Favours formal financial system	Favours cash carriers or informal financial systems such as Hawala and currency exchange firms.	Formal financial system is preferred up until the point of entry when the money is taken out in cash in a neighbouring country and carried into a country that poses a high PF risk e.g. the Democratic People's Republic of Korea. Additionally, the use of distributed ledger technology has become a widely used mechanism

			to settle transactions for DPRK because of its decentralised nature.
Detection Focus	Suspicious transactions such as deposits uncharacteristic of customer's wealth or the expected activity	Suspicious relationships, such as wire transfers between seemingly unrelated parties	Individuals, entities, states, goods and materials, activities
Transaction Amounts	Large amounts often structed to avoid reporting requirements	Small amounts usually below reporting thresholds	Moderate amounts
Financial Activity	Complex web of transactions often involving shell or front companies, offshore secrecy havens, etc.	Varied methods including formal banking systems, informal value transfer systems, smuggling of cash and valuables	Transactions look like normal commercial activity, structured to hide connection to proliferator or proliferations activities
Money Trail	Circular money eventually ending up with the person who generated it	Linear money trail; generated money is used to propagate terrorist groups and activities	Linear money trail: money is used to purchase goods and materials from brokers or manufacturers. The money can also move in the opposite direction (i.e., from the broker/manufacturer to the proliferator).

STAGES OF TERRORIST FINANCING

The Terrorist Financing process typically involves three stages: raising, moving, and using funds and other assets.

Methods of raising funds to finance terrorism

The basic need of terrorists is to raise, move and use funds. Terrorism fundraising methods vary based on the sophistication and the aim of the terrorist organisations. Small groups and individual actors may require only modest amounts of money, which are more difficult to detect through AML/PTF transaction monitoring systems. Organisations with a larger support base require larger amounts of funding to support more sophisticated organisational structures and ongoing operational costs. These greater costs may require the use of larger scale and more organised fundraising methods. Key channels used to raise funds for terrorism financing include:

(i) **Raising funds from legitimate sources:** Terrorist organisations receive considerable support and funding from and through legitimate sources including NPOs, businesses, and through self-funding by terrorists and their associates from employment, savings, and other means.

- *NPOs:* NPOs or non-profit organisations possess characteristics that make them particularly attractive to terrorists or vulnerable to misuse for terrorist financing. They enjoy the public trust, have access to considerable sources of funds, and their activities are often cash intensive. Furthermore, some NPOs have a global presence that provides a framework for national and international operations and financial transactions, often in or near areas most exposed to terrorist activity. Finally, NPOs are subject to significantly lighter regulatory requirements than financial institutions or other businesses, (for example, for starting capital, professional certification or background checks for staff and controllers at registration, or for ongoing record keeping, reporting and monitoring), depending on the country and legal form of the NPO and reflecting their principally nonfinancial role.
- *Legitimate Businesses:* The proceeds of legitimate businesses can be used as a source of funds to support terrorist activities. This is a particular risk in sectors which do not require formal qualifications, or where starting a business does not require substantial investments. The risk that a business will divert funds to support terrorist activity is greater where the relation between sales reported and actual sales is difficult to verify, as is the case with cash-intensive businesses.
- *Self-Funding:* In some cases, terrorist groups have been funded from internal sources, including family and other non-criminal sources. The amounts of money needed to mount small attacks can be raised by individual terrorists and their support networks using savings, access to credit or the proceeds of businesses under their control. Terrorist organisations can be highly decentralised, and self-funding can include cases in which a relatively autonomous external financial facilitator who is not directly involved in planning or carrying out an attack nevertheless contributes funding.

(ii) **Raising funds from criminal proceeds:** FATF reports have indicated that terrorist organisations engage in a variety of illegal activities to generate funds. Criminal activity can generate large sources of funds reasonably quickly, making it attractive to terrorist groups. Small cells and individual sympathisers may turn to crime if they have no other significant source of income or wider support network. Terrorist financiers use FIs to raise funds mainly via credit card fraud and cheques fraud. More specifically:

- *Credit Card Fraud:* Credit cards are highly vulnerable to misuse for terrorist financing purposes and other illegal activities. There is a market for illegally obtained personal details, including credit card account numbers, as well as personal information such as the card holder's full name, billing address, telephone number, start and expiry dates, the security number on the rear of the card, etc.
- *Cheques Fraud:* Chequebook fraud allows terrorists to raise and move significant amounts of cash quickly. Several cases have been identified in which a basic model of bank fraud has been applied to generate funds for terrorism. These cases involved bank accounts being opened using false identity documents and

fraudulent deposits. Organised individuals are likely to carry out this activity by drawing cheques from the same account simultaneously in several locations.

Methods of moving funds to finance terrorism

There are three main methods by which terrorists move money or transfer value. The first is through the use of the financial system, the second involves the physical movement of money (for example, through the use of cash couriers), and the third is through the international trade system.

(i) Financial System

- Financial institutions and other regulated financial service providers represent the formal financial sector and serve as the principal gateway through which retail and commercial transactions flow. Additionally, the services and products available through the formal financial sector serve as vehicles for moving funds that can support terrorist organisations and fund acts of terrorism. The speed and ease with which funds can be moved within the international financial system allow terrorists to move funds efficiently and effectively and often without detection between and within jurisdictions.
- Combined with other mechanisms such as offshore corporate entities, formal financial institutions can provide terrorists with the cover they need to conduct transactions and launder proceeds of crime when such activity goes undetected.
- All financial institutions used to move funds are potentially vulnerable to TF by facilitating illicit fund transfers, including funds transfers through banks and Money or Value Transfer System (MVTS) mechanisms.

(a) Funds Transfers Through Banks

- The banking sector continues to be the most reliable and efficient way to move funds internationally and remains vulnerable to TF. Several FATF reports have referred specially to the use of the bank accounts of NPOs to move funds to terrorist organisations.
- The banking sector is an attractive means for terrorist groups seeking to move funds globally because of the speed and ease at which they can move funds within the international financial system. The sheer size and scope of the international financial sector gives terrorist groups and financiers the opportunity to blend in with normal financial activity to avoid attracting attention.
- AML/PTF mitigation measures put in place by financial institutions are likely making it more difficult to move terrorist funds through the financial sector; however, the risk remains. Traditional products can be abused for terrorist financing. For example, sympathisers of a terrorist group can open savings accounts and provide the debit card associated with the account to a member of the terrorist organisation to enable them to access cash via withdrawals from overseas bank ATMs.

(b) Money or Value Transfer Systems (MVTS)

- Along with the banking sector, the remittance sector has proven to be particularly attractive to terrorists for funding their activities and has been exploited to move illicit funds.
- Radical groups as well as persons related to terrorist organisations have used the network of the registered and worldwide operating money transfer companies to send or receive money.
- Migrant communities and families rely heavily on MVTS to remit funds home; this provides a channel for commingling TF with legitimate family transfers. It also makes it difficult to detect TF from normal family and community remittances.
- Advances in payment system technology have had a twofold impact on the potential abuse by terrorist financiers of such systems. Electronic payment systems allow law enforcement an increased ability to trace individual transactions through electronic records that may be automatically generated, maintained and/or transmitted with the transaction. However, these advances also create characteristics that may be attractive to a potential terrorist. For instance, the increased speed and volume of funds transfers - in the absence of the consistent implementation of standards for recording key information on such transactions, maintaining records, and transmitting necessary information with the transactions - could serve as an obstacle to ensuring traceability by investigative authorities of individual transactions.

(ii) Physical Movement of Money

- The physical movement of cash is another way terrorists can move funds without encountering the AML/PTF safeguards established in FIs and DNFBPs. Terrorists and their supporters have converted cash into high-value and hard-to-trace commodities such as gold or precious stones in order to move assets outside of the financial system. International counter-terrorist operations have shown that cash couriers have transferred funds to a number of countries within the Middle East and South Asia. Direct flight routings are used for simple transfers; however, indirect flight routings using multiple cash couriers and changes in currencies take place within more sophisticated schemes.
- While funds may be raised in a number of ways, often they are converted into cash to be taken to conflict zones. This is assisted by porous national borders, difficulty in detecting cash smuggling (particularly in the small amounts that are sometimes smuggled for TF purposes), and the existence of informal and unregulated economies. The increase of bulk cash smuggling across borders between conduit countries and high-risk areas has also been noticed.

(iii) Trade System

- The international trade system is subject to a wide range of risks and vulnerabilities, which provide terrorist organisations the opportunity to transfer value and goods through seemingly legitimate trade flows. For example, the over- and under-

invoicing of goods and services, is one of the oldest methods of transferring value across borders, and it remains a common practice today. It is accomplished by misrepresenting the price of a goods or services in order to transfer money between colluding importers and exporters.

TF THREATS TO THE TCI

The TCI's 2017 National Risk Assessment (NRA) found that the risk of TF was low in the TCI. The NRA revealed that the TCI was not near any areas of conflict and that there was no known link to the financing of terrorism or support for terrorism among the population in the TCI. The evaluation also noted that there was no significant business or trade relations with countries or regions with high terrorist threats and other conditions that could pose a threat to the TCI. There have been no suspicious activity reports filed against an NPO, FI, DNFBP nor have their controllers, directors or senior officers faced criminal prosecution.

On this basis TF threats to the TCI are likely to be external from state actors and non-state actors that seek to exploit the TCI's financial system, non-profit organisations, financial services businesses, or gatekeepers, to clandestinely finance, procure, ship, or trans-ship goods for use in the commission of terrorist acts outside of the TCI.

The TCI, as an international financial centre, has a financial services sector that attracts foreign customers; this characteristic contribute to higher TF risks. While there is currently no evidence to suggest that TCI regulated entities are involved in terrorist financing activities, the exposure of the TCI's financial system when conducting business in the international financial markets poses TF risks.

VULNERABILITIES TO TF

While terrorist financing has not been identified as currently a high risk in the TCI's National Risk Assessment, this does not mean the financial system cannot be vulnerable to terrorist financing. Based on international typologies, terrorist financiers usually provide or collect funds or assets at places such as:

- non-profit organisations
- banks and money or value transfer businesses
- lawyers and trust and company service providers; and
- when moving physical cash across borders using formal or informal money remittance services.

Sectoral Vulnerabilities

NPO sector

The NPO sector can be a potential channel for raising and distributing funds for terrorism financing. NPOs can be misused to raise funds to finance or support terrorist acts (with or without the NPO's knowledge) through:

Using NPO funding

For example, a local organisation that has a relationship with the NPO to conduct project activities overseas, a 'partner organisation,' uses all or part of the NPO's money to fund acts of terrorism.

Using NPO assets

For example, the NPO's vehicles or premises are used to transport or store weapons.

Using the NPO's name and status

For example, fundraising is conducted in the name of the NPO by a terrorist organisation, without the NPO's knowledge or consent.

Committing financial abuse within an NPO

For example, members of a terrorist group may infiltrate the NPO and pose as employees, who then skim off money from fundraising to fund terrorist purposes.

Setting up an NPO for illegal or improper purposes

For example, a terrorist group registers an NPO, but the NPO does not work towards their charitable purpose. The group uses all of the NPO's funds for terrorism financing.

The factors that allow NPOs to achieve outcomes and gain trust and respect from the public also make them vulnerable to being misused to fund terrorism.

Operating locations

- NPOs may have a global presence that provides a framework for national and international operations and financial transactions.
- NPOs are known to work within or near areas that are most exposed to terrorist activity.
- NPOs may operate in emergencies or provide humanitarian responses in locations where there are no banks or infrastructure, and they may have to deal in cash or use alternative remittance systems.

Financial operations

- NPOs can have complex financial operations which are not always accounted for in detail, including:
    - multiple donors, investments, and currencies
    - a high volume of small transactions
    - informal money transfers.
- There may be unpredictable and unusual income and expenditure streams, so suspicious transactions may be hard to identify.

Organisational structure and programs

- NPOs may be run by one or two key individuals, often in unsupervised roles which makes it easy to quickly move money and assets around.
- There can be complex programs of operation and some NPOs may pass funds through intermediary partner organisations to deliver their services.

The high level of public trust

- NPO activities may not be scrutinised as consistently as other sectors.

Banks and money or value transfer sectors

These sectors are vulnerable because they can be used by terrorist financiers to access the international financial system to process payments for the benefit of terrorists from overseas sources.

Trust and company service providers, independent legal professionals, accountants

These sectors are used for creating legal persons and legal arrangements (or assisting in their creation and operation) that terrorist financiers may use to obscure the links between a financial transaction and terrorist benefactors. Legal persons and legal arrangements can have ownership and control exercised through nominees.

Dealers in precious metals and stones

These sectors can provide an alternative method for terrorist financiers to surreptitiously move financial resources across international borders. It is easy to melt gold bullion and convert it into different forms to disguise the fact that it is gold. For example, there have been media reports about the interdiction of gold shipments between North and South America where the gold was disguised as American souvenirs. There have also been instances of gold being reshaped into cones and common items such as wrenches, nuts, bolts and belt buckles. Gold in these forms is easier to conceal from border authorities and its value can be considerably understated on the Bills of Lading.

The maritime sector

Given the challenges with securing borders, designated persons and entities can exploit the maritime sector to deliver weapons and other materials for use in terrorist acts.

PREVENTATIVE MEASURES

Terrorist financing can be mitigated by risk assessment of customers and products, application of customer due diligence measures, including enhanced due diligence on high-risk customers and transactions.

Risk Assessment of FIs and DNFBPs

Given that criminals may exploit FIs and DNFBPs to finance terrorists, FIs and DNFBPs must adopt a risk-based approach to managing their TF risks. To apply a risk-based approach, FIs and DNFBPs will need to understand TF risks based on the risk factors for ML and TF which are listed below:

i) the organisational structure of the FI/DNFBP, including the extent to which it outsources activities;

ii) the persons to whom and how the FI/DNFBP delivers its products and services;

iii) the countries with which the FI/DNFBP customers are connected;

iv) the products and services that the FI/DNFBP provides or offers to provide;

v) the nature, scale, and complexity of the activities of the FI/DNFBP;

vi) reliance on third parties for elements of the customer due diligence process; and

vii) new business practices and new or technological developments for new and existing products

A detailed guide explaining the steps to be taken to carry out a proper business risk assessment is set out in the Commission's Guidelines on Risk Assessment.

Application of CDD Measures

The application of CDD measures is integral in the AML/PTF framework of FIs and DNFBPs. Knowledge of the customer helps to understand the general activities in which the customer would usually be expected to engage. As part of their due diligence process, FIs and DNFBPs must:

1. Obtain customer due diligence information on every customer, third party and beneficial owner comprising—

    (a) identification information in accordance with regulation 14 of the AML Code, which must include:
        (i) the full legal name of the customer, any former names and any other names used by the customer;
        (ii) the gender of the individual;
        (iii) the principal residential address of the individual;
        (iv) the date of birth of the individual

    (b) relationship information in accordance with regulation 12 which must include:
        (i) the purpose and intended nature of the business relationship;
        (ii) the type, volume and value of the expected activity;
        (iii) the source of funds and - where the customer risk assessment indicates that the customer, business relationship or occasional transaction presents a high risk - the source of wealth of the customer, third party or beneficial owner;
        (iv) details of any existing relationships with the company;

(v) the reason for using a company based in the TCI where the customer is not resident in the TCI; and

(vi) such other information concerning the relationship that, on a risk-sensitive basis, the company considers appropriate.

2. Consider, on a risk-sensitive basis, whether further identification or relationship information is required

3. Based on the information obtained through identification and relationship information (including where obtained through enhanced due diligence measures), prepare and record a risk assessment with respect to the customer. The customer risk assessment must particularly consider the relevance of the following risks—
   (a) customer risk;
   (b) product risk;
   (c) delivery risk; and
   (d) country risk.

4. Verify the identity of the customer; and

5. Periodically update the customer due diligence information that it holds and adjust the risk assessment that it has made accordingly

The Commission's DNFBP Customer Due Diligence Guidance provides more information on the application of CDD measures, including the enhanced due diligence measures that should be taken for high-risk customers.

Staff Training

It is the responsibility of FIs and DNFBPs to remain abreast and current regarding TFS risks, maintain and execute suitable mitigation measures, and to ensure that all employees are adequately informed and trained on the relevant policies, processes, and procedures.

Non-Profit Organisations

Strong governance arrangements and internal controls within NPOs can reduce the risk of an NPO being used for terrorist financing. The Commission has published guidance (please see guidance at https://tcifsc.tc/non-profit-organizations-policies-guidelines/) for the NPO sector that require NPOs to establish governance standards, operate lawfully, and be run in an accountable and responsible way.

Additionally, the NPO Regulation requires NPOs to keep the following records for a period of at least five years:

i) their purpose, objectives and activities;

ii) the identity of the persons who control or direct their activities, including, as appropriate, senior officers, directors and trustees;
iii) the identity, credentials and good standing of its beneficiaries and associate NPOs;
iv) financial records that show and explain its transactions, within and outside the TCI, and that are sufficiently detailed to show that its funds have been used in a manner consistent with its purposes, objectives, and activities, and show the source of its gross annual income; and
v) a list of donors who have donated in excess of $10,000 as a single donation or cumulatively, during the year.

NPOs must also report financial information annually to the Commission which adds to the accountability and transparency of NPOs.

ANNEX 1 – Terrorist Financing Indicators

Terrorism financing indicators are often indistinguishable from money laundering indicators. Terrorism financing often, but not always, involves smaller amounts of money than when illicit criminal funds are laundered. Funds intended for terrorism may also be derived from legitimate rather than illicit sources, making terrorism financing more difficult to detect.

The presence of a single indicator may not necessarily raise a suspicion but could warrant further monitoring and examination. Multiple indicators are more likely to result in a suspicion being formed. Additionally, an FI's overall knowledge of a customer, including the customer's established financial transaction history, can be as important as any of the indicators below in forming a suspicion of terrorism financing.

Terrorism financing indicators include, but are not limited to, the following:

- Structured[1] cash deposits and withdrawals, and international funds transfers to high-risk jurisdictions. These transactions may be conducted at multiple branches of the same reporting entity;
- Multiple customers conducting international funds transfers to the same beneficiary located in a high-risk jurisdiction;
- A customer conducting funds transfers to multiple beneficiaries located in the same high-risk jurisdiction;
- A customer using incorrect spelling or providing variations on their name when conducting funds transfers to high-risk jurisdictions;
- Transfer of funds between business accounts and personal accounts of business officeholders which is inconsistent with the type of account held and/or the expected transaction volume for the business;
- Large cash deposits and withdrawals to and from NPO accounts;
- Operating a business account under a name that is the same as (or similar to) a name used by listed entities locally and overseas;
- Individuals and/or businesses transferring funds to listed terrorist entities or entities reported in the media as having links to terrorism;
- Funds transfers from the account of a newly established company to a company selling chemicals that could be used in bomb making;
- Multiple low-value domestic transfers to a single account and cash deposits made by multiple third parties, which could be indicative of fundraising for terrorism financing;
- Sudden increase in account activity, inconsistent with customer profile;

[1] 'Structuring' is a money laundering technique, which involves the deliberate division of a large amount of cash into a number of smaller deposits or transfers (including international funds transfers) to evade reporting requirements or other scrutiny.

- Multiple cash deposits into a personal account described as 'donations' or 'contributions to humanitarian aid' or similar terms;
- Transfers through multiple accounts followed by large cash withdrawals or outgoing funds transfers overseas;
- Multiple customers using the same address and telephone number to conduct account activity; and
- Prohibited entities or entities suspected of terrorism using third-party accounts (for example, a child's account or a family member's account) to conduct transfers, deposits or withdrawals.