COMBATING THE FINANCING OF TERRORISM

GUIDANCE FOR FINANCIAL INSTITUTIONS

NOVEMBER 2020

Table of Contents

I. PURPOSE, SCOPE, AND APPLICABILITY

- This guidance paper produced by the Central Bank of Bahrain (CBB) should be read in conjunction with the pertinent local and international standards. It touches upon key issues identified by FATF in relation to the role of financial institutions in combating the financing of terrorism. Therefore, financial institutions are urged to comprehensively read FATF issued guidance papers on the same subject. The paper is applicable to all licensees regulated and supervised by the CBB.

- The paper is aimed at providing guidance on the private sector's obligations under the United Nations Security Councils (UNSCR) in relation to combating the financing of terrorism (CFT). In addition, the paper addresses indicators of potential terrorist financing.

- The paper was developed by consolidating relevant information applicable to financial institutions, including preventive measures from the guidance papers and typologies issued by the Financial Action Task Force (FATF).

- This guidance paper refers to information provided in the following guidance and typologies:

  - FATF Targeted Financial Sanctions Related to Terrorism and Terrorist Financing (Recommendation 6) issued in **June 2013**

  - FATF 'International Best Practices - Targeted Financial Sanctions Related to Terrorism and Terrorist Financing (Recommendation 6) issued in **June 2013**

  - FATF Emerging Terrorist Financing Risks issued in **October 2015**

  - Wolfsberg Guidance on Sanctions Screening issued in **January 2019**

  - FATF Report – Terrorist Financing Risk Assessment Guide – **July 2019**

II. INTRODUCTION

Given the apparent threats posed by terrorists and terrorist organizations, financial institutions are required to include combating the financing of terrorism (CFT) measures as an integral part of their compliance programs commensurate with the Terrorism Financing (TF)risks identified as part of the FIs' TF Risk Assessment.

TF threats may include domestic or international terrorist organizations and their facilitators, their funds, as well as past, present, and future TF activities. Moreover, it includes small terrorist cells or individual terrorists capable of committing attacks and significantly harming society.

Certain measures must be adopted by jurisdictions to assist financial institutions in combating terrorist financing. These include implementing targeted financial sanctions (TFS) programs, protecting vulnerable sectors, including the charitable sector and money-service businesses, and encouraging effective reporting of suspicious activity. The term targeted financial sanctions means both asset freezing and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of designated persons and entities.

Terrorists use a wide variety of methods to move money within and between organizations, including the financial sector, the physical movement of cash by couriers, and the movement of goods through the trade system. Charities and alternative remittance systems have also been used to disguise terrorist movement of funds. The adaptability and opportunism shown by terrorist organizations suggests that all the methods that exist to move money around the globe are, to some extent, at risk. A clear understanding of the TF process is required by financial institutions in order to effectively combat terrorist financing, including understanding the methods used to raise and move terrorist funds, scenarios indicating possible TF activities, and the emerging TF risks.

III. IMPLEMENTATION OF TERRORIST FINANCING CONVENTIONS

- Recommendation 6 requires each country to implement targeted financial sanctions to comply with the United Nations Security Council resolutions that require countries to freeze, *without delay*, the funds or other assets, and to ensure that no funds and/or other assets are made available to or for the benefit of:
  (i) any person or entity designated by the United Nations Security Council (the Security Council) under Chapter VII of the Charter of the United Nations, as required by Security Council resolution 1267 (1999) and its successor resolutions; or
  (ii) any person or entity designated by that country pursuant to Security Council resolution 1373 (2001).

- As defined by FATF, the phrase *without delay* means, ideally, within a matter of hours of a designation by the United Nations Security Council or its relevant Sanctions Committee (e.g., the 1267 Committee, the 1988 Committee, the 1718 Sanctions Committee). For the purposes

of S/RES/1373 (2001), the phrase without delay means upon having reasonable grounds, or a reasonable basis, to suspect or believe that a person or entity is a terrorist, one who finances terrorism or a terrorist organization. In both cases, the phrase without delay should be interpreted in the context of the need to prevent the flight or dissipation of funds or other assets which are linked to terrorists, terrorist organizations, those who finance terrorism, and to the financing of proliferation of weapons of mass destruction, and the need for global, concerted action to interdict and disrupt their flow swiftly.

- The focus of Recommendation 6 is on the preventive measures that are necessary and unique in the context of stopping the flow of funds or other assets to terrorist groups, and the use of funds or other assets by terrorist groups.

- Effective freezing regimes are critical to combating the financing of terrorism and, as a preventive tool, accomplish much more than freezing terrorist-related funds or other assets present at any particular time. Effective freezing regimes also combat terrorism by:

  (a) Deterring non-designated persons or entities who might otherwise be willing to finance terrorist activity;

  (b) Exposing terrorist financing "money trails" that may generate leads to previously unknown terrorist cells and financiers;

  (c) Dismantling terrorist financing networks by encouraging designated persons or entities to disassociate themselves from terrorist activity and renounce their affiliation with terrorist groups;

  (d) Terminating terrorist cash flows by shutting down the pipelines used to move terrorist-related funds or other assets;

  (e) Forcing terrorists to use more costly and higher risk means of financing their activities, which makes them more susceptible to detection and disruption; and

  (f) Fostering international co-operation and compliance with obligations under the pertinent sanctions regimes.

IV. FINANCIAL INSTITUTIONS OBLIGATIONS AND MEASURES TO COMBAT TERRORISM FINANCING

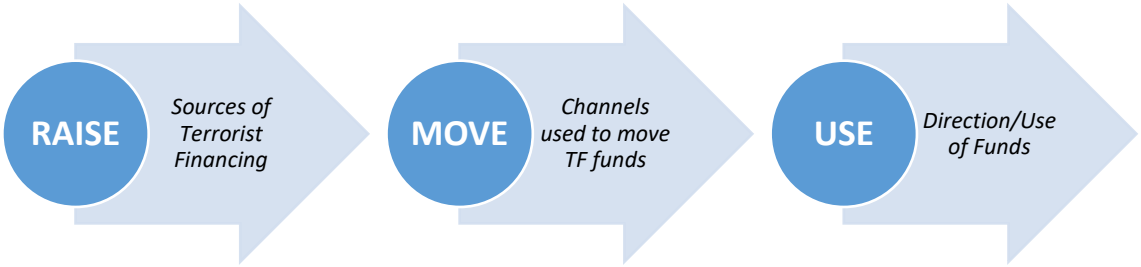
In order for financial institutions to be able to effectively monitor, detect and report TF activities to the competent authorities, they are required to have in place the following measures as a minimum:

- Incorporate TF risk as part of the financial institution's overall AML/CFT Risk Assessment. The financial institution should identify and assess the TF risks to which it is exposed given the nature, size, complexity and geography of its business.
- Design and implement specific measures to mitigate the TF risks identified, as well as procedures for TF activities monitoring, detection and reporting to the relevant authorities.

- As part of their TF combating measures, all financial institutions are required to conduct sanctions screening in order to detect, prevent, and manage risks arising from dealing with persons listed under the applicable sanctions regimes. Implementing an effective screening process assists with the identification of sanctioned individuals and organizations, as well as potential illegal activities to which FIs may be exposed. It helps to identify areas of potential sanctions concern and supports compliance teams in making appropriately informed risk decisions.
- Two main screening controls are to be used by FIs in order to achieve their objectives: (a) transaction screening and (b) customer screening. Transaction screening is used to identify transactions involving targeted individuals or entities, whereas customer screening is designed to identify targeted individuals or entities during customer on-boarding i.e. prior to establishing a business relationship, and through the lifecycle of the customer relationship with the FI.
- There should be documented procedures that clearly define the mechanisms used by the financial institution to screen customers and transactions versus applicable sanctions lists pertaining to TF activities. This includes procedures for updating the lists in a timely manner in situations of new listings and de-listing and reporting of positive name matches.
- Include TF monitoring and detection as part of the overall Compliance Program and job descriptions of the relevant compliance staff.
- Ensure that the relevant staff are trained and kept up to date on TF risks, activities and their respective responsibilities.

V. STAGES OF TERRORIST FINANCING

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



- In order to effectively combat TF, FIs are likely to undergo an analysis stage, which involves a consideration of the different sources, channels, destinations and origins of terrorist funds and other assets:

    - **Sources of terrorist financing**: Funds are raised through various means, such as through donations, self-funding, or criminal activity. The sources of financing are likely to differ between different terrorist actors – for example, the value and sources of funding for foreign terrorist fighters is likely to differ from the sources used to fund large terrorist organizations.

    - **Channels**: Terrorist financiers use different channels to move funds and assets to a terrorist network, organization, or cell, such as through the banking sector, money service business (MSB) sector, cash smuggling, informal remittances, etc.

    - **Direction/Use of funds**: Funds or other assets might be generated by terrorist financiers in the home jurisdiction, but used by terrorists for operations elsewhere or vice versa. Alternatively, funds or other assets may transit through the jurisdiction for use elsewhere. The funds are typically used to purchase weapons or bomb-making equipment, for payment to insurgents, or to cover living expenses for a terrorist cell.

- Funds used to finance terrorism are considered an 'instrument of crime' (which are either illicit or legitimate funds directed towards a criminal purpose). In this way, funds used to finance terrorism are similar to funds used in the commission of most other crimes (for example, a payment for a drug shipment). The three-stage process described above can also describe the flow of money involved in other crime types. However, one significant difference between terrorism financing and other crime types is that most terrorism financing originates from ostensibly legitimate sources and activities.

- Crucially, the factors associated with TF risk are also distinct from those associated with money laundering (ML) risk. While laundered funds come from the proceeds of illegal activities, funds used to finance terrorism may come from both legitimate and illegitimate sources. Similarly, for ML it is often the case that the generation of funds may be an end in itself with the purpose of laundering being to transmit the funds to a legitimate enterprise. In the case of TF, the end is to support acts of terrorism, terrorist individuals and organizations, and for that reason the funds or other assets must, for the most part, ultimately be transferred to persons connected with terrorism. Another important distinction is that while identification of ML risk is often enforcement-led, TF risk by the nature of the threat will need to be more intelligence led.

- Although there may be some overlap in the potential vulnerabilities that criminals and terrorists misuse, the motive, and therefore the threat and risk indicators, differs. While transfer of a low volume of funds may be lower risk for ML, this type of activity may pose a higher risk indicator for TF when considered along with other factors (e.g. reporting thresholds or limited amount of funds necessary to carry out terrorist acts). For example,

terrorist financiers have been known to use low-limit prepaid cards for TF purposes despite being considered lower risk for ML *(see Section VIII – Emerging TF Threats).*

VI. METHODS OF RAISING FUNDS TO FINANCE TERRORISM

- While the number and type of terrorist groups and related threats have changed over time, the basic need for terrorists to raise, move and use funds has remained the same. However, as the size, scope and structure of terrorist organizations have evolved, so too have their methods to raise and manage funds.

- Terrorism fundraising methods vary based on the sophistication and the aim of terrorist groups. Smaller groups and individual actors may require only modest amounts of money, which are more difficult to detect through AML/CFT transaction monitoring systems. Groups with a larger support base require larger amounts of funding to support more sophisticated organizational structures and ongoing operational costs. These greater costs may require the use of larger scale and more organized fundraising methods. Key channels used to raise funds for terrorism financing include:

    (i) **Raising funds from legitimate sources:** Terrorist organizations receive considerable support and funding from and through legitimate sources including charities, businesses, and through self-funding by terrorists and their associates from employment, savings, and social welfare payments. This includes the phenomenon known as "blackwashing" where legal funds, for example money stemming from collection by charities or social benefits, are diverted for purposes of radicalization, recruitment or terrorism.

        - *Charities:* Charities or non-profit organizations 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 charities 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, charities are subject to significantly lighter regulatory requirements than financial institutions or publicly-held corporate entities, (for example, for starting capital, professional certification or background checks for staff and trustees at registration, or for ongoing record keeping, reporting and monitoring), depending on the country and legal form of the charity and reflecting their principally non-financial 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 organizations can be highly decentralized, 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 organizations 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. In particular, small cells and individual sympathizers 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. Organized individuals are likely to carry out this activity by drawing cheques from the same account simultaneously in several locations.

VII. 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 support terrorist organizations 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 organizations.

  - 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/CFT 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, sympathizers of a terrorist group can open savings accounts and provide the debit card associated with the card to a member of the terrorist organization 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.

- MVTS operations range from the large-scale and regulated funds transfer mechanisms[1] available in the formal financial sector, to small-scale alternative remittance systems. Radical groups as well as persons related to terrorist organizations 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 rapidity 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 one way terrorists can move funds without encountering the AML/CFT safeguards established in financial institutions. Known groups 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. 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.

[1] Funds transfers refer to any financial transaction carried out for a person through a financial institution by electronic means with a view to making an amount of money available to a person at another financial institution.

- 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 organizations the opportunity to transfer value and goods through seemingly legitimate trade flows. In recent decades, international trade has grown significantly: in 2019, world merchandise exports exceeded USD 18 trillion a year, and world commercial services trade accounted for a further USD 6.03 trillion[2].

VIII. SCENARIOS INDICATING POSSIBLE TF ACTIVITIES

- 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[3] 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;

[2] World Trade Organization (2019)

[3] '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.

- 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;

- 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.

IX. EMERGING TF RISKS

- Emerging risks are defined as new and unforeseen risks whose potential impact is not fully known or rapidly evolving. There are certain TF risks that are evolving rapidly, such as foreign terrorist fighters (FTFs), social media, new payment products and services, and the exploitation of natural resources.

(i) Foreign Terrorist Fighters (FTFs)

- The FTF phenomenon is not new, but the recent scaling up of individuals travelling to Iraq and Syria has been a challenge for many FATF members. FTFs are predominantly using traditional methods, particularly self-funding, to raise the funds they require to travel to the conflict areas.

- The United Nations Security Council Resolution (UNSCR) 2178 raises concern about the establishment of international terrorist networks, which is relevant considering the range of countries that FTFs originate from.

- While FTFs are not presently considered to be a significant source of funding for ISIL or Al-Nusrah Front (ANF), they contribute to the larger TF threat posed by these groups. More importantly, FTFs are considered one of the main forms of material support to terrorist groups, and thus remain a significant TF threat. Self-funding by individuals and funding by recruitment/facilitation networks are assessed as the two most common methods used to raise funds for FTFs.

(ii) Social Media

- The role of social media in breeding violent extremism has been well reported but less is known about how it is used to raise funds for terrorists and terrorist groups.

- There are significant vulnerabilities associated with social media, including anonymity, access to a wider range and number of potential sponsors or sympathizers and the relative ease with which it integrates electronic payment mechanisms. It is also apparent that donors are often unaware of the end-use of funds supported by social media, including crowdfunding, which presents a risk that terrorist organizations can exploit.

(iii) New Payment Products and Services

- Methods of TF continue to evolve in response to changes in technology or deliberate attempts to circumvent law enforcement CFT efforts. Electronic, online and new

payment methods pose a vulnerability, which may increase over the short term as overall use of these systems, grows. Many of these systems can be accessed globally and used to transfer funds quickly. A number of online payment systems and digital currencies are also anonymous by design, making them attractive for TF, particularly when the payment system is based in a jurisdiction with a comparatively weaker AML/CTF regime.

- *Virtual Currencies:* Virtual currencies have emerged and attracted investment in payment infrastructure built on their software protocols. These payment mechanisms seek to provide a new method for transmitting value over the internet. At the same time, virtual currency payment products and services (VCPPS) present ML/TF risks. Virtual currencies such as bitcoin, while representing a great opportunity for financial innovation, have attracted the attention of various criminal groups, and may pose a risk for TF. This technology allows for anonymous transfer of funds internationally. While the original purchase of the currency may be visible (e.g., through the banking system), all following transfers of the virtual currency are difficult to detect. The US Secret Service has observed that criminals are looking for and finding virtual currencies that offer anonymity for both users and transactions, the ability to move illicit proceeds from one country to another quickly, low volatility that results in lower exchange risk, widespread adoption in the criminal underground, and reliability.

- *Prepaid Cards:* While there are a wide variety of prepaid cards, the category of card of most concern is open-loop cards where funds can be withdrawn at Automatic Teller Machines (ATMs) worldwide. These network-branded payment cards allow transactions with any merchant or service provider participating in the payment network (e.g. Visa or MasterCard). General Purpose Reload (GPRs) cards are financial products that consumers can apply for online or pick-up from the prepaid section at various retailers. These cards are activated later by the consumer by phone or online. These products function like any other bank-issued debit card. In terms of TF risk, these cards can be loaded domestically via cash or non-reportable electronic methods and carried offshore inconspicuously with no requirement to declare their movement across the border. On arrival in a high-risk country or transit country for TF, the funds are then converted back to cash through multiple offshore ATM withdrawals, restricted only by ATM withdrawal limits. Once a loaded card has been carried offshore, funds are accessible with minimal chance of detection.

- *Internet-Based Payment Services:* Internet-based payment services provide mechanisms for customers to access, via the Internet, prefunded accounts that can be used to transfer the electronic money or value held in those accounts to other individuals or businesses, which also hold accounts with the same provider. Recipients may or may not be required to register with the payment service provider to receive a funds transfer. The extent to which these

transactions have been used to finance terrorism is unclear. Some TF cases involving low-value transactions via online payment systems such as PayPal have also been linked to a number of terrorism suspects. Terrorism suspects have been observed using multiple online payment accounts, combining both verified and guest accounts. Payments appear to be linked to online purchases of equipment and clothing prior to the departure of individuals travelling to conflict zones rather than direct payments to associates to fund terrorist activities.

- *Exploitation of Natural Resources:* The ability to reap high rewards from the natural resources sector coupled with the weak institutional capability, particularly in or near areas of conflict, creates a significant vulnerability for terrorist organizations to capitalize on. The exploitation of natural resources is considered a subset of how terrorist organizations control and occupy territory. This issue is also linked to how terrorist organizations fund themselves through criminal activity and through potential links to organized crime groups. Criminal activity related to this sector includes extortion, smuggling, theft, illegal mining, kidnapping for ransom, corruption and other environmental crimes. Terrorist organizations could use these resources as a means to raise funds by controlling or exploiting a wide variety of vulnerable resources to include gas, oil, timber, diamonds, gold (and other precious metals), wildlife (e.g., ivory trading) and charcoal (e.g., in Somalia). These sectors represent a profitable source of revenue and may also be appealing because of weak regulation in the sector.

X. OVERALL CONCLUSIONS

- While terrorist organizations are continuing to adapt and counter law enforcement responses, it is clear that they continue to require resources to meet their destructive goals. Following the financial trail and a good understanding of how all types of terrorist organizations, whether large territorially based or small cells operating autonomously, need, use and manage funds is critical in detecting, preventing and sanctioning terrorist and terrorist financing activity.

- This guidance paper is intended to assist financial institutions in supporting the implementation of robust CFT systems, which take into account changing TF risks, trends and methods. The FATF Recommendations and related interpretations and guidance provide the necessary AML/CFT framework to address the TF risks identified in this paper, but effective implementation of these standards is key.