Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Justice and Police FDJP

Federal Office of Police fedpol
Crime Prevention and Legal Affairs
Money Laundering Reporting Office Switzerland

CH-3003 Bern
fedpol, MROS

Bern, 05.12.2023

ADDENDUM TO THE ALERT

dated November 3, 2023 in the context of the terrorist attacks by Hamas and Palestinian Islamic Jihad (PIJ) on Israel on October 7, 2023

TABLE

1. INTRODUCTION

Money laundering and terrorist financing know no national borders and the ways and methods, criminals use to launder their money or transfer money in order to fund terrorist activities evolve constantly and quickly. Therefore, cooperation is key between the different actors in the 'chain' to increase consistency, efficiency, and actionable response to emerging ML/TF threats. Private partners have a role and legal obligation to detect and report unusual or suspicious transactions to their national financial intelligence units (FIU). The Money Laundering Reporting Office Switzerland (MROS) at fedpol is Switzerland's FIU and central money laundering office. MROS receives and analyses suspicious activity reports in connection with money laundering, terrorist financing, money of criminal origin or criminal organisations and, where necessary, forwards them to a range of law enforcement agencies to facilitate existing or start new investigations. Those investigations need to lead to a convincing number of successful prosecutions and finally recovered assets as proceeds from crime. This kind of 'threat intelligence information' should provide the financial intermediaries more insights and overall situational awareness to improve the detection, analyses, prevention, and investigation of financial and economic crime, including new threats. This document is the result of the international collaboration of MROS analysing and taking into consideration not only observations from the public, but also from the private sector.

The purpose of this document is to provide information on typologies and indicators relating to financing of terrorist organizations. While this document focuses on the financing of terrorist organisations, certain typologies may also apply to the financing of individual terrorists or small terrorist cells.

This document does not claim to be exhaustive and provides only a sample of typologies and indicators on the financing of terrorist organisations. It is intended to supplement the information already available to the public and private sectors.

2. CONTEXT

On October 7, 2023, a series of terrorist attacks from Hamas and the Palestinian Islamic Jihad (PIJ) on Israel resulted in the death of over 1'400 persons[1]. It appears that the most *modus operandi* used by Hamas and the PIJ are common to those used by terrorist organizations more generally. For this reason, it was decided to compile some of the available typologies and indicators on terrorist organizations and include them in this document.

Even if there is no internationally accepted standard definition of terrorism, there appears to form widespread consensus concerning what a terrorist act actually is, namely a deliberate assault on civilians or civilian property with the aim of intimidating ordinary people or pressurising a state or international organisation into acting in a certain way or refraining from action.[2] According to the FATF glossary[3], terrorist financing (TF) is the financing of terrorist acts, and of terrorists and terrorist organizations.

A terrorist act includes:

(a) an act which constitutes an offence within the scope of, and as defined in one of the following treaties: (i) Convention for the Suppression of Unlawful Seizure of Aircraft (1970); (ii) Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1971); (iii) Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents (1973); (iv) International Convention against the Taking of Hostages (1979); (v) Convention on the Physical Protection of Nuclear Material (1980); (vi) 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); (vii) Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (2005); (viii) Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf (2005); (ix) International Convention

---

1 Federal Council condemns terrorist attacks by Hamas in Israel and enhances Switzerland's capacity to act (admin.ch): On November 22, 2023 the Federal Council decided to propose a federal Act to Parliament banning Hamas in Switzerland (Federal Council decides to bring in legislation to ban Hamas (admin.ch).

2 Countering terrorism (admin.ch)

3 https://www.fatf-gafi.org/en/pages/fatf-glossary.html

for the Suppression of Terrorist Bombings (1997); and (x) International Convention for the Suppression of the Financing of Terrorism (1999).

(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 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. Financing of terrorism means, in a simplified way, to financially support terrorism. It can be done by sending or receiving money or property in various ways that are intended to finance terrorism, but also to be used by a terrorist organization. The funds do not have to be used for a specific attack, but can also be used, for example, for training, materials, or the purchase of equipment.

To better detect suspicious transactions or behaviour which could be linked to TF, it is important to know the key elements of TF. First, TF can be divided in three stages:

- The raising of funds, through illicit or licit activities,
- The moving of funds,
- The use of funds.

TF not only involves direct financing of acts of terrorism, but also financing of propaganda, recruitment, training, travel, daily living expenses and other operational needs.

The collection of funds can take place in many different ways, for example through deposits into accounts for private individuals, NPOs, foundations or companies. The funds can be transferred abroad through various payment service providers or unregistered Hawala intermediaries.

Since TF is an ever-evolving crime, it is of the utmost importance to establish mechanisms particularly tailored for the obliged entities' business to monitor TF risk regularly and on an ongoing basis, taking into account contemporary terrorism and TF developments and threats. Subject persons should therefore ensure that they remain up to date with information on emerging TF trends, guidance documents, and reports issued by reputable international bodies and organizations.

The indicators mentioned below are not specific to one TF stage and can therefore be found in different stages. As no single red flag is determinative of illicit or suspicious activity, obliged entities should consider the totality of available information and circumstances, such as a customer's historical financial activity, whether the transactions are in line with prevailing business practices, and whether the customer exhibits multiple red flags, before determining that a behaviour or transaction is suspicious.

For an overview of the EU terrorism situation and trends, please refer to the Europol document "EU Terrorism Situation & Trend Report (TE-SAT)"4. From a Swiss point of perspective, according to the Federal Intelligence Service (FIS), the terrorist threat in Europe, including Switzerland, remains acute. The threat from terrorism has become unpredictable. It emanates primarily from radicalised individuals who commit acts of violence using the simplest modi operandi, such as knife or vehicle attacks. Potential perpetrators include persons radicalised in Switzerland, returnees from conflict zones or jihadists released from prison. Terrorists sometimes also use Switzerland as a logistical base for planning attacks in other countries or as a transit point.[5]

3. MODUS OPERANDI

3.1. CASH

Even if criminals continually use new technologies to transfer funds, cash remains an important *modus operandi* among terrorist groups and organizations. Physical coins and banknotes are used in different ways to finance terrorism. Cash can be deposited into banking accounts, used as mean of payment or used to purchase value instruments or materials. Funds are especially transferred via cash couriers or postal services. Cash is commonly used, as it provides several advantages:

- Anonymity;
- Transportation across borders;
- Difficult to trace;
- No audit trail;
- The most common and traditional method in the black market.

4 https://www.europol.europa.eu/publications-events/main-reports/tesat-report
5 Terrorism – Current situation (admin.ch)

3.2. NON-PROFIT ORGANIZATIONS

Non- Profit Organizations (NPOs) may be abused by terrorists due to the enjoyed public trust, access to funds and cash insensitivity. NPOs are more vulnerable to be misused since they are usually subject to lighter regulatory requirements, as opposed to other financial institutions or corporate entities.

Many NPOs have a global presence, facilitating national and international operations and financial transactions. The highest risk lies within the NPOs which operate in or close to highly exposed TF areas and move funds from or to these countries.

There are different scenarios that demonstrate how NPOs may be abused for TF.

- Firstly, diversion of funds or fraud within legitimate NPOs, where persons donate money to organizations that are set up for legitimate charitable purposes. The donations are transferred to the place of need by the NPO, but rather than going to the intended purposes, funds are diverted to terror activities;
- Sham organizations are used to pose as a legitimate NPO as a front organization for a terrorist group. In such cases, financial institutions and other service providers would unknowingly be providing their services to terror financiers and/or terror networks. Likewise, people donating funds believe to spend their money for a legitimate charitable project;
- Broad exploitation, where charitable organizations, such as purpose foundations or voluntary organizations, intentionally raise funds for persons in a third country who form part of or support a terrorist organization;
- NPOs making bank transfers to other NPOs known to be involved in terrorist activity or TF.

For additional information, please refer to the recent document from the FATF on "Best Practices on Combating the Abuse of Non-Profit Organisations"[6].

[6] https://www.fatf-gafi.org/en/publications/Financialinclusionandnpoissues/Bpp-combating-abuse-npo.html

3.3. CROWDFUNDING

Crowdfunding inherently relies on the goodwill of supporters to donate to a particular initiative. Humanitarian, charitable, and non-profit causes can serve as effective covers for financial solicitation and can be abused for TF purposes. Terrorist groups may be motivated to raise funds through crowdfunding because it is a relatively quick and simple way to obtain donations from supporters across the world. Donations-based crowdfunding is the most vulnerable to TF abuse given its characteristics.

Criminals publish fraudulent humanitarian appeals, often in absence of a registered charitable organization to finance terrorism. In this modus operandi, individuals purport to be raising funds for charitable purposes, such as providing social or medical support or building infrastructure projects. Moreover, funds can be solicited under the cover of community activities, such as false sporting events. Funds can be raised via social media or formal donation crowdfunding platforms. The campaign promoters themselves may also be affiliated with a terrorist group.

Alternatively, fundraising campaigns can be organized by, or affiliated to, sham charity organizations that are operating as front entities for terrorist groups. The sham organization does not undertake humanitarian relief but is instead involved in illegal activity and finances terrorism.

Social media sites and online messaging services enable users to connect with local or global communities and to disseminate their message. Social media platforms play a key role in a crowdfunding campaign and are by consequence used strategically by terrorists for TF purposes. Criminals share campaign links and payment instructions with their followers, recruit supporters, share advice on how to avoid detection, and take advantage of features like encryption to transmit sensitive details. Sophisticated algorithms on social media direct users to content based on their search history, which in the context of terrorism can intensify the shared terrorism-based content.

For additional information, please refer to the recent document from the FATF on "Crowdfunding for Terrorism Financing"[7].

[7] https://www.fatf-gafi.org/en/publications/Methodsandtrends/crowdfunding-for-terrorism-financing.html

3.4. CRYPTOCURRENCIES

Cryptocurrencies pose an increasing risk for TF. Virtual assets service providers (VASP) may be used to transfer and/or exchange funds from fiat currency to virtual assets (VA)s. VAs can be used as a means of payment within black markets, or on the Darknet for the purchase of illicit material. VAs may also be withdrawn in cash from crypto-ATMs, or exchanged to fiat currency and subsequently withdrawn and the received funds are used to support terror activities.

To increase anonymity, criminals use privacy coins such as Dash and Monero, protecting the identity and ensuring the coin user's anonymity. They often use unhosted wallets for direct funding or fundraising purposes to overcome the matter of AML/CTF checks by Crypto Asset Service Providers.

The use of "mixers" increases the TF risk as it blends cryptocurrencies of many users together to obfuscate origins and owners of the funds. It further increases privacy of cryptocurrency transactions and the difficultly to trace the users and the related transactions.

Crypto assets might be used in a hybrid way, which means in combination with another product either provided by the financial sector or from other service providers such as IVTS services, banking services, TCSP services or NPO services.

Terrorist groups have used social media platforms like Facebook and Twitter to publicly share their crypto wallet addresses and provide instructions on how to make donations. Recent examples also show that messaging systems such as WhatsApp, Telegram or Signal are being used to call for donations.

There are also known cases of ransomware attacks for TF purposes, in which victims are forced to move funds to specific VA wallet addresses to regain access to the stolen data.

3.5. UNREGULATED SYSTEMS

Informal Value Transfer Systems (IVTSs) like Hawala are methods for criminals to move funds around the world under the supervisory radar. In Hawala banking, the

international money audit trail is eliminated since the funds do not actually cross borders.

Funds are transferred by coded information, such as an identifiable number, and cross various portals of choice, like online chats, text messages, e-mails, or letters. Hawala agents use in general advanced protected internet technology, which eliminates manual accounts and record-keeping evidence. The receiver gets a telecommunication confirmation with an identifiable number to pick up the funds in the designated country.

IVTSs are difficult to identify, as the persons involved normally operate within or in addition to a legitimate and/or front business.

For additional information, please refer to the document from the FATF on "The role of Hawala and other similar service providers in money laundering and terrorist financing"[8].

3.6. USE OF CORPORATE VEHICLES

Criminals try to hide the origin or ownership of their assets and funds by setting up complex networks of corporate structures, including limited partnerships or legal arrangements, such as trusts, in various jurisdictions, including offshore jurisdictions. Such networks of corporate structures may include shell or front companies designed to obscure ownership, sources of funds, destination of funds, reason of the transfer and the countries involved in the financial transactions. The networks of companies are mainly used to execute international wire transfers, often involving financial institutions in jurisdictions distinct from those of the companies' registered office. Such entities may lack or have minimal physical and online presence.

By using regulated offshore trust and TCSP services, it is possible to incorporate a company in a specific jurisdiction to make investments such as the purchase of a significant property and/or the settlement of assets into a tax efficient structure. Through this newly incorporated company or the purchase of a property, criminals can

[8] https://www.fatf-gafi.org/en/publications/Methodsandtrends/Role-hawalas-in-ml-tf.html

finance terrorist activities. It is possible to have the same scenario with legal arrangements like trusts, in which funds from the trust may have been diverted and potentially used for TF purposes.

For additional information, please refer to the document from the FATF on "Concealment of Beneficial Ownership"[9].

3.7. DOMESTIC FUNDING

Some terrorist groups have direct access to state funds or receive funds through taxation in the areas they control (e.g. Hamas). This can range from import taxes to a form of income tax on citizens. For instance, Hamas collects taxes on good coming from Egypt to Gaza such as cigarettes, fuel, and construction materials. In 2022, the organization imposed new taxes on imported West Bank products.

3.8. DIASPORA AND IDENTITY-BASED NETWORKS

Some terrorist groups have large diaspora and identity-based networks around the world. This phenomenon plays a role in various conflict regions. These networks and the corresponding support can be done under different forms. These are often wealthy individuals, who support terrorist groups from abroad. Some provide funds from illegal activities, taking advantage of the lax regulations in countries where they are based. They are a prime target for fundraising campaigns.

3.9. USE OF HIGH-RISK JURISDICTIONS

Criminals can circumvent weak AML/CFT controls to successfully finance terrorist activities through the financial system. High-risk regions can be conflict areas, countries bordering conflict zones, countries suffering from terrorist attacks, countries with large diasporas from high-risk jurisdictions and countries with weak AML/CFT regimes and weak central governance[10]. High-risk regions are frequently used as transfer countries and/or destination country. Persons or business held by persons of

[9] https://www.fatf-gafi.org/en/publications/Methodsandtrends/Concealment-beneficial-ownership.html
[10] Please also refer to the FATF black and gray lists: https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html

the same origin as the high-risk countries move funds to their origin country, which are later used to finance terrorism.

In general, geographical risks associated with source, destination and transit countries should always be taken into consideration when assessing TF risks.

4. INDICATORS AND CASE STUDIES

4.1. KNOW YOUR CUSTOMER INDICATORS

Know your customer ("KYC") indicators include each element, which is in relation to the client, such as customer identification and verification, understanding the nature and purpose of the business relationship, beneficial ownership identification and verification, source of wealth and source of funds verification, as well as the customer's behaviour.

KYC indicators might be the following:

- The customer's identity
    - The customer is mentioned on sanctions lists directly applicable in the reporting entity's jurisdiction (i.e. Hamas, PIJ, Hizballah Military Wing);
    - The customer is mentioned in adverse media articles (open source), or referenced in CDD tools;
    - The customer is linked to entities or individuals mentioned on sanctions lists, or mentioned in adverse media articles (open source), or referenced in CDD tools;
    - The customer is associated with a high-risk jurisdiction;
    - The customer operates in areas and jurisdictions that are known to be used by terrorist organisations to finance their activities;
    - The customer operates in a sector that is known for high TF risks;
    - Suspicious behaviour of the customer, for example reluctance to provide KYC or KYT information, avoiding personal contact, insisting on using an intermediary, avoiding communication after the formal entry into relationship or handing out forged/altered documentation;
    - The customer provides misleading CDD documentation;

- The entity has only recently been incorporated and has no financial trading history;
- IP addresses that do not correspond to a customer's reported location data or that are in areas of conflict;
- Customer using an IP address associated with a darknet or other similar software that allows anonymous communication, including encrypted emails and VPNs.

- Doubts about beneficial ownership

  Given the existing sanctions lists and CDD tools, it is difficult for a terrorist organisation to enter direct business relations with regulated entities. These organisations therefore try to conceal their true identity by using front men or complex legal structures. The following indicators may help to identify the concealment of beneficial ownership.
  - Use of false corporations, including shell-companies;
  - Use of nominees, trusts, family member or third party accounts;
  - The legal structures used do not seem to make any economic sense;
  - Beneficial owner of the account not properly identified;
  - The customer's wealth, lifestyle, behaviour or transactions is not consistent with the customer's profile;
  - Doubts about the supporting documents on the origin of funds;
  - The client seems to be living beyond his means.
- Customer behaviour after the beginning of the business relationship
  - Conducting a large initial deposit to open a new relationship, while the amount funded is inconsistent with the customer profile;
  - A safe deposit box 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;
  - A new user attempts to trade the entire balance of VAs, or withdraws the VAs and attempts to send the entire balance off the platform.

Case study 1: Use of corporate vehicles

Client X portrays himself as a successful entrepreneur from West Africa with a vast business empire specialising in the commercial production and export of charcoal to

the Middle East and more recently diversifying into the extraction of high value minerals again in East Africa. Client X is introduced to a regulated offshore Trust and Company Service Provider ("TCSP") with a view to incorporating a company to purchase a significant property in "European City 1" and settling the asset into a tax efficient structure. Client X also seeks to settle funds into a trust structure to fund the education of his children. As the relationship with the TCSP develops further, Client X seeks to incorporate further companies to manage new business ventures in Africa, including road haulage and shipping. Client X regularly pays the feared terrorist group Al-Shabaab a tax for all charcoal and minerals exported. In addition, he pays protection money to Al-Shabaab to ensure that his road haulage and shipping assets remain free from interference. In short, Client X through his trading companies helps fund the terrorist activities of Al-Shabaab.

Indicators

- The client is associated with a high-risk jurisdiction.
- The TCSP is providing services to a trading company.
- The charcoal trade is a known source of funding for the Al-Shabaab Group

Case study 2: NPOs / Trusts

A regulated offshore Corporate Service Provider delivers services to a Private Fund ("PF").

The PF as a private investment fund involving the pooling of capital raised for the fund and which operates on the principle of risk spreading. A review of the Beneficial Owner of a Middle Eastern corporate investor, "Company P" identified a philanthropic donation to an educational facility in a Middle East jurisdiction with links to a terrorist group. The proposed investor owned an offshore administered legal arrangement (Trust) and his source of funds for the Trust was derived from established family wealth in the Middle East. The Settlor of the Trust was also identified as administering a philanthropic fund, which donated annually to several local education facilities.

Indicators

- The Middle East jurisdiction was a high-risk jurisdiction with links to TF.
- Adverse media reporting suggested that there was direct support to a terrorist group linked to the education facility.

Case study 3: TF scenario for the fund & TCSP sector

Client X is the Settlor of a Trust in a regulated offshore jurisdiction, which is administered by a Trust and Company Service Provider ("TCSP"). The Trust was established for the benefit of Client X's extended family. A sole non-familial beneficiary "Client Y" was appointed to the Trust. Client Y is resident in a high-risk country in the Middle East and is a close family friend of the Settlor and is entrusted to make distributions from his own funds on behalf of the Trust to family members who are not named beneficiaries of the Trust, but who are also resident in high-risk jurisdictions with strong links to TF. Client Y is then re-imbursed by the Trust through "European country 1" based bank accounts held in his own name. Enhanced checks reveal that Client Y's associated businesses and his immediate family operate a network of currency exchange businesses based both in "European country 1" and in a number of linked high-risk jurisdictions. These checks also reveal that some of Client Y's family members and their family linked businesses are also subject to sanction measures for supporting terrorist organisations including The Islamic State. Therefore, concerns have been formed that funds from the Trust may have been diverted and potentially used for TF purposes.

Indicators

- The appointment of a non-familial beneficiary based in a high-risk jurisdiction associated with TF
- Operation of a network of currency exchange businesses in high-risk jurisdictions
- The use of both a formal banking system and a suspected informal value

system (potentially money services businesses/Hawala type arrangements) to facilitate the funds to individuals not named as beneficiaries of the Trust.

- Although not directly sanctioned, Client Y maintains close familial and business links with individuals and businesses who are subject of sanction measures.
- An audit trail in respect of the final destination of the distributions made to Client Y under the guise as a "beneficiary" could not be established.

Case study 4: TF scenario for the fund & TCSP sector

An offshore regulated Financial Services Business provide administration services for a "European country 1" registered fund, which in turn owns an investment holding company, which in turn owns a "European country 2" registered company, which is the sole lender to a "European country 1" registered privately-owned property group, "Client X" which holds investments in properties operating across the Hotel sector.

This multimillion-pound loan is secured against a real estate asset – a hotel based in "European city 1".

Client X receives a non-binding offer to purchase the "European city 1". Hotel through a "European city 1" based independent (regulated) investment firm from a recently registered "European country 1" company "Company W". This offer would have been sufficient to settle the outstanding capital and interest on the loan, which was reported to be slightly less than the asking price. This prompted a due diligence exercise, which revealed adverse media relating the UBO of Company W who was identified as being an "Client P", an Iranian National who was resident in "Middle East country 1" where he also held business interests. These adverse media checks confirmed that Client P was a member of Iran's Islamic Revolutionary Guard Corps and was involved in the facilitation of the movement of gold from a South American country through to the Middle East, where it was converted into currency to allegedly finance Hezbollah terrorist activities. A suspicion was subsequently formed that the "European city 1" hotel may have been purchased with the proceeds of money laundering/ TF and axiomatically if the hotel was to be purchased by Client P the income derived from the hotel may in turn be used for TF purchases. In addition, if

the Fund were to receive the proceeds from the sale of the hotel to settle the loan, then in turn there is a likelihood that these funds could taint the remaining fund which could have been subject of potential freezing orders, which ultimately would have affected the underlying investors investment.

Indicators

- "European country 1" Company registry checks reveal that Client P's name, and his date of birth were not accurately recorded, and a suspicion was formed that this was done intentionally.
- Checks on the registered "European country 1" address for Company W revealed a generic residential street address that was associated with numerous unconnected company entities.
- Open-source checks confirm that Company registry has not been able to prevent companies from providing false information.
- Company W had only recently been incorporated and had no financial trading history.
- Client P's "Middle East country 1" based company had links to an associated company in Iran, which owned a oil tanker, which was subject of Iranian sanctions violations.
- Adverse media revealed that Client P was circumventing sanction measures and being involved in providing TF to sanctioned terrorist organisations.

4.2. TRANSACTIONAL INDICATORS

Transactional indicators are mainly based on unusual payment patterns, complex payment structures, transactions involving suspicious persons or jurisdictions or all other suspicious transactions:

- Open-source information / the environment in which transactions are carried out
    - A request to transfer funds to terrorist organizations or a request to transfer funds to an entity or organization that is linked to those organizations;

- An entity which begins to receive donations from donors, which have previously donated to terrorist organizations, entities linked to those organizations or an entity whose activity was frozen;
- Crypto addresses, bank accounts, digital payment means etc. published on the terrorist organizations' affiliated social media platforms or having links to such platforms;
- Use of phrases and numbers in the transfer of funds, where there is an indication that they are related to terrorism in general or in the context of current events. For example, money transfers to organizations whose names indicate a link to terrorism such as the name of a famous martyr or a word such as "Jihad" or a stated purpose to assist the fighting in conflict zones (i.e. Gaza);
- Payments made through a website with the initial appearance of legitimacy, but closer examination reveals indications of connections to a terrorist organization;
- Transacting with VA addresses or bank cards that are connected to known sanctioned addresses, terrorist organizations clusters, entities or individuals linked to such clusters or illegal fundraising campaigns.

- Justification / reason of the transactions (absence of a business rationale)
  - No business rationale or economic justification for the transactions;
  - Activity appearing on an account that is consistent with a previous pattern of activity on an account controlled by a relative or other related party which has since been blocked;
  - A series of complicated transfers of funds from one person to another as a means to hide the source and intended use of the funds;
  - Multiple cash deposits and withdrawals with suspicious references;
  - Unexplained third-party payments being received regularly;
  - Unexplained periods of account dormancy;
  - Deposits were structured below the reporting requirements to avoid detection;
  - Multiple cash deposits in small amounts in an account followed by a large wire transfer to another country;
  - Frequent electronic money transfers followed by the depletion of funds through transfers to third parties;

    - Transferring VAs immediately to multiple VASPs, especially to VASPs registered or operated in high risk jurisdictions;
    - Depositing VAs at an exchange and then withdrawing the VAs without any additional exchange activity;
    - Converting a large amount of fiat currency into VAs;
    - Transactions making use of mixing and tumbling services;
    - The explanations given by the customer regarding suspicious transactions are misleading / the customer refuses to give any explanations;
    - The transactions could be linked to the evasion of sanctions (i.e. against a high-risk jurisdiction).
- Inconsistencies with the client's profile
    - Transactions which are inconsistent with the account's normal activity;
    - Change in the customer's behaviour;
    - Transaction activity on a personal account is indicative of operating an unregistered NPO, with a large number of cash or wire donations funding onward transfers to family members or other related accounts;
- Purpose of the transactions
    - Opening an account and immediately after engaging in extensive financial activity for humanitarian purposes;
    - Usage of financial services as alternative transfer channels;
- Links to high-risk jurisdictions
    - Outgoing transactions to high risk jurisdictions;
    - Use of ATMs in high-risk jurisdictions or in areas bordering conflict zones;
    - Retailers in a high-risk jurisdiction receiving regular, round amount transfers via MSBs from overseas remitters, where the value or regularity of the payments is inconsistent with expectations for that retailer's line of business;
    - Transactions involving foreign currency exchanges are followed within a short time by funds transfers to higher-risk locations;
    - Funds are generated by a business owned by persons of the same origin or by a business, which involves persons of the same origin from high-risk countries.

Case study 5: Use of the funds

Client A has a long-standing banking relationship and an unremarkable banking history. Since retiring from the armed services on medical grounds he has dedicated much of his time to supporting a far-right wing extremist group ("the Group") and regularly raises funds for the Group by way of selling memorabilia and organising training sessions for members in remote locations. Such training includes weapons training and bomb making skills. The Group advocate violent direct action against any organisation that helps to support illegal migrants into the country. In recent times, the Group have focused their attention on community leaders and politicians seeking to intimidate and drive their agenda. Client A uses his bank account to receive third party payments for the sale of the memorabilia and attendance at the weapons training events. Payments are made to hire venues for the training events. He also posts pictures of himself wearing paramilitary clothing and carrying a firearm advertising the next training session. The volume of third-party payments into a personal bank account causes concern at the bank. When challenged by bank staff, client A claims that the funds received from third parties represent income derived from trading on an online marketplace. Client A is subsequently arrested at a violent demonstration and charged with violent disorder and the unlawful association.

Indicators

- Change in banking activity.
- Unexplained third-party payments being received regularly.
- The photographs posted on the website.
- Payments made to secure training venues.
- Client A concealing the true reason for the third-party payments

4.3. FUNDRAISING INDICATORS

Fundraising indicators can be any form of financial support for a terrorist organization, either directly or indirectly through individuals or entities linked to these organizations.

Fundraising indicators are not limited to the collection of money but also to the organization or campaign itself:

- Inconsistencies regarding the beneficiary of a fundraising campaign
    - A fundraising campaign that mimics and uses an existing charity/initiative as a front to raise funds for TF;
    - A non-transparent fundraising campaign with unclear recipient of the donations, fundraising through natural person accounts linked to high-risk jurisdictions;
    - Activity on an account consistent with charitable fundraising but the recipient has not registered as a charity in the jurisdiction of operation, or its registration has been suspended or cancelled;
- NPO related indicators
    - Recent date of incorporation of the NPO;
    - Designation and objectives of NPO might be unclear;
    - The use of funds by the non-profit organization is not consistent with the purpose for which it was established;
    - Multiple personal and business accounts or the accounts of NPOs or charities are used to collect and funnel funds to a small number of foreign beneficiaries;
    - The non-profit organization has little or no staff, which is suspicious considering its stated purpose and expected financial activity;
    - An address given by the NPO or its affiliates, which belongs to or is used by organizations suspected of terrorist activity;
    - Evidence that NPO donors, partners, suppliers or beneficiaries are involved themselves or are related to entities involved in terrorist activity.

5. MANAGING THREAT RESPONSE ACTIVITIES

For the purpose of better detecting terrorism financing, additional coverage of established transaction surveillance might be useful within the industry:

- Screening of open-source information and social media;
- Checks for inconsistencies in Customer Due Diligence (CDD) information;
- Update CDD information / enhanced CDD;
- Immediate cooperation with the FIU / law enforcement;

- Awareness campaigns through national and international public-private partnerships;
- Exchange of strategic information via public-private partnerships domestically and internationally;
- Take advantage of public databases to crosscheck information about PEPs, their affiliates and family members in case of adverse media news.

6. REPORTING TO MROS

With that respect, we would like to underline the importance of Article 9 para 1 AMLA which says, that a financial intermediary must immediately file a report with MROS if it knows, or has reasonable grounds to suspect that assets involved in the business relationship are subject to the power of disposal of a criminal or terrorist organization, or serve the financing of terrorism.[11]

7. FURTHER READING

- FATF, Best Practices on Combating the Abuse of Non-Profit Organisations, November 2023 Best Practices on Combating the Abuse of Non-Profit Organisations (fatf-gafi.org)
- FATF, Crowdfunding for Terrorism Financing, October 2023 Crowdfunding for Terrorism Financing (fatf-gafi.org)
- FATF, Detecting Terrorist Financing – Relevant Risk Indicators, July 2019 Terrorist Financing Risk Assessment Guidance (fatf-gafi.org)
- FATF, Virtual Assets – Red Flag Indicators, September 2020 Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing (fatf-gafi.org)
- FATF, Concealment of Beneficial Ownership, July 2018 Concealment of Beneficial Ownership (fatf-gafi.org)
- FATF, The role of Hawala and other similar service providers in money laundering and terrorist financing, October 2013 The role of Hawala and other similar service providers in money laundering and terrorist financing (fatf-gafi.org)
- Europol, EU Terrorism Situation & Trend Report (TE-SAT), June 2023 EU Terrorism Situation & Trend Report (TE-SAT) | Europol (europa.eu)

[11] SR 955.0 - Federal Act of 10 October 1997 on Combating Money Laundering and Terrorist Financing in the Financial Sector (Anti-Money Laundering Act, AMLA) (admin.ch)

8. LIST OF ABBREVIATIONS

AML/CTF: Anti-Money Laundering and Countering the Financing of Terrorism
CDD: Customer Due Diligence
FIU: Financial Intelligence Unit
IVTSs: Informal Value Transfer Systems
KYC: Know your customer
ML/TF: Money Laundering and Terrorism Financing
MSB: Money Services Business
NPOs: Non-Profit Organizations
PEP: Politically Exposed Person
PIJ: Palestinian Islamic Jihad
TCSP: Trust and Company Service Provider
TF: Terrorism Financing
VA: Virtual Assets
VASP: Virtual Asset Service Provider