FIAU

Guidance Document on

The Funding of Terrorism

A GUIDANCE DOCUMENT ISSUED BY THE FIAU ON EMERGING TRENDS, TYPOLOGIES AND RED FLAGS RELATED TO THE FUNDING OF TERRORISM

Issued: 07 February 2018
Revised: 27 November 2020

CONTENTS

ABBREVIATIONS 4

PREFACE 5

1. INTRODUCTION TO FUNDING OF TERRORISM 6

1.1 FUNDING OF TERRORISM IN MALTESE LAW 8

1.2 MONEY LAUNDERING VERSUS FUNDING OF TERRORISM 9

1.3 HOW DOES FUNDING OF TERRORISM TAKE PLACE? 10

1.4 FUNDING OF TERRORISM IN MALTA 11

1.4.1 Flow-through 13
1.4.2 Service providers 14
1.4.3 Abuse of philanthropic organisations 14
1.4.4 Local case studies 15

2. TYPOLOGIES AND EMERGING TRENDS IN FT 21

2.1 CASH 22

2.1.1 Vulnerabilities 22
2.1.2 Red flags 22

2.2 FUND TRANSFERS AND MONEY REMITTANCE 23

2.2.1 Vulnerabilities 23
2.2.2 Red flags 25

2.3 VIRTUAL FINANCIAL ASSETS 26

2.3.1 Vulnerabilities 26

2.3.2 Red flags 27

2.4 LOANS 28

2.4.1 Vulnerabilities 28

2.4.2 Red Flags 28

2.5 NON-PROFIT ORGANISATIONS AND CHARITIES 29

2.5.1 Vulnerabilities 29

2.5.2 Red Flags 32

2.6 LEGAL PERSONS AND ARRANGEMENTS 33

2.6.1 Vulnerabilities 33

2.6.2 Red Flags 34

2.7 TRADE-BASED TERROR FINANCING 35

2.7.1 Vulnerabilities 35

2.7.2 Red Flags 37

3. EMERGING FT TRENDS IN MALTA 39

CONCLUDING REMARKS 40

ABBREVIATIONS

AML	Anti-Money Laundering
ATM	Automated Teller Machine
BO	Beneficial Owner
CDD	Customer Due Diligence
CFT	Countering the Funding of Terrorism
EU	European Union
FIAU	Financial Intelligence Analysis Unit
FIU	Financial Intelligence Unit
FT	Funding of Terrorism
IVTS	Informal Value Transfer System
ML	Money Laundering
NCC	National Co-ordinating Committee on Combating Money Laundering and Funding of Terrorism
NPO	Non-Profit Organisation
PMLFTR	Prevention of Money Laundering and Funding of Terrorism Regulations
SMB	Sanctions Monitoring Board
STR	Suspicious Transaction Report
TF RA	Terrorism Financing Risk Assessment
VFA	Virtual Financial Asset

PREFACE

One of the objectives that the Prevention of Money Laundering and Funding of Terrorism Regulations ('PMLFTR') seeks to achieve is combatting the Funding of Terrorism ('FT'). Subject persons play a key role in ensuring that the financial system and the services of professionals and certain designated businesses are not misused to fund terrorism. To this end, subject persons who know, suspect or have reasonable grounds to suspect that a transaction may be linked to funding of terrorism must submit a report to the Financial Intelligence Analysis Unit ('FIAU') as set out under Regulation 15(3) of the PMLFTR.

The consequences of FT can be disastrous, and so, when a transaction is flagged for suspicion of FT, this should be escalated and assessed as quickly as possible so that a Suspicious Transaction Report ('STR') can be filed promptly with the FIAU. Likewise, when the FIAU receives such an STR, it is handled with urgency and assigned the highest level of priority.

In order to detect and report suspicions, subject persons need to be sensitive to transactions, patterns or behaviour that is indicative of FT.

In February 2018, the FIAU issued its 'Guidance Note on Funding Of Terrorism – Red Flags and Suspicious Activities'. This document provided a list of activities, patterns or behaviours that are indicative of potential FT.

In 2019, the National Co-ordinating Committee on Combating Money Laundering and Funding of Terrorism (NCC) carried out a Terrorism Financing Risk Assessment (TF RA) to assess the risks of FT in Malta. The TF RA was adopted in December 2019 and is an essential tool for competent authorities to recognise weaknesses and prioritise efforts in a risk-sensitive manner. Findings from these risk assessments are equally useful for subject persons, who can refer to the results thereof when informing their risk understanding and developing proportionate and effective controls.

This Guidance Document on the Funding of Terrorism combines insights and select findings from the 2019 TF RA and builds on the FIAU's 2018 Guidance Note by providing more substantive information on emerging trends and typology-specific case studies and red flags. The document is divided into three Chapters:

- Chapter 1 introduces the topic of FT, by defining and setting out the activities that comprise of FT and provides an overview of Malta's inherent vulnerabilities relating to the movement of funds;
- Chapter 2 looks at different typologies and red flags associated with various products and services, with case studies from across the globe; and
- Chapter 3 contains a list of red flags based on emerging trends identified in Malta.

1. INTRODUCTION TO FUNDING OF TERRORISM

Crimes have nowadays become increasingly complex since they may be interconnected and global, and take place on both physical and virtual levels. Terrorists and terrorist financiers have adapted to the counter-measures being implemented by states, and have responded by becoming more creative, expanding and varying their methods to raise and move funds, and this is why the fight against FT is as critical as the fight against terrorists themselves.

FT is a global phenomenon that threatens a country's security, economic development, reputation and financial market stability. In the words of former 9/11 Chief of the FBI's Counter-Terrorism Financing Operations Section Dennis M. Lormel: "Funding is both the lifeblood of a terrorist organisation and one of its most significant vulnerabilities."

Since terrorist groups require financial support to carry out their activities and achieve their goals, choking off the money that flows to these groups interferes with their ability to conduct terrorist attacks. It must be borne in mind that the funds accumulated by terrorist financiers are not solely used to fund the material used to conduct terrorist acts, but also for operational, educational and recruitment expenses, apart from charitable undertakings that may appear legitimate but which, when carried out by these persons, fall within the scope of FT.

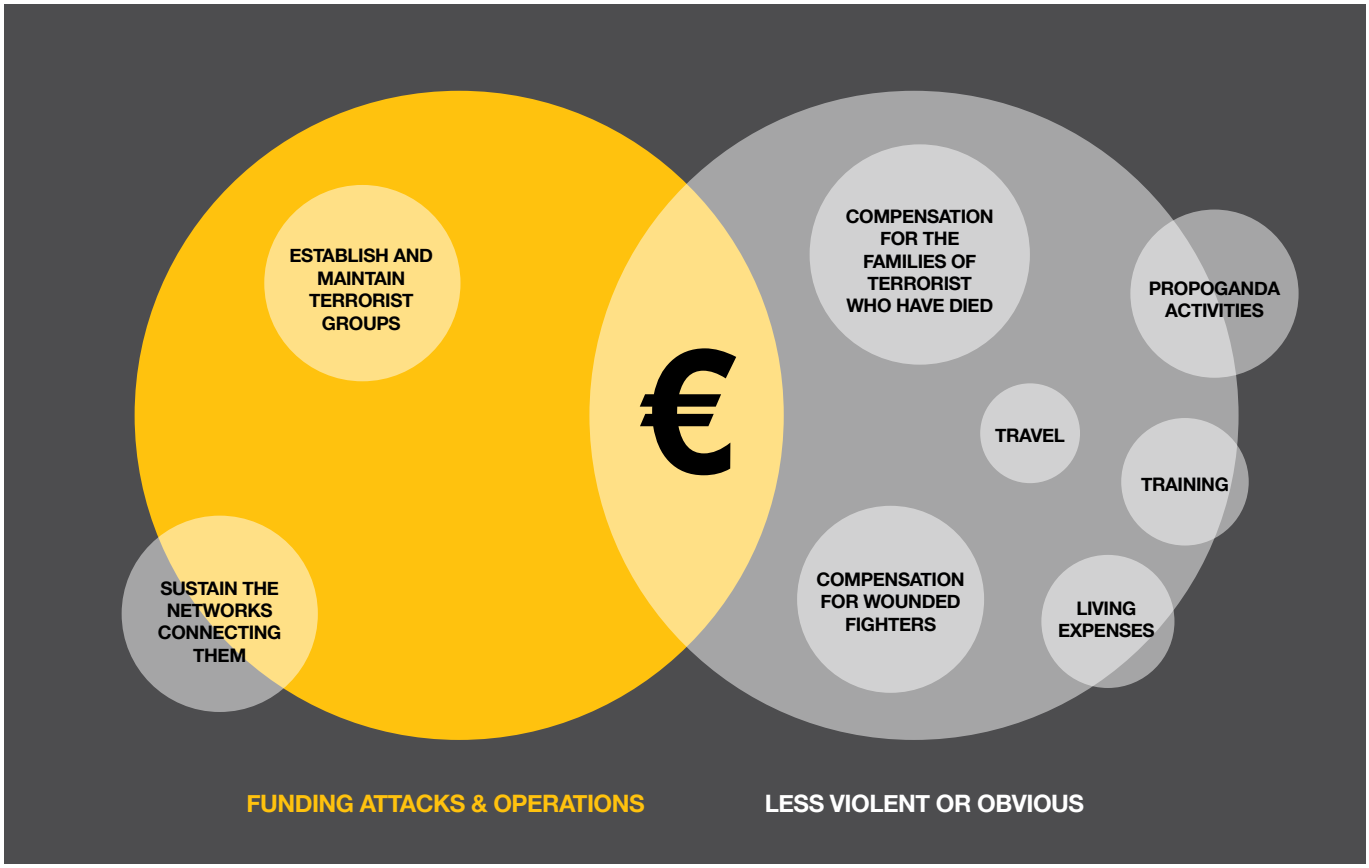


Figure 1 – reproduced from "Building a profile: Financial Characteristics Associated with Known Foreign Terrorist Fighters and Supporters" AUSTRAC

It must also be borne in mind that, just because terrorism does not appear to be prominent in a jurisdiction, this does not mean that the jurisdiction is not being used to assist with funding purposes. Since without funding, terrorist networks cannot operate, it is of the essence for subject persons to act as gatekeepers to the financial industry by identifying the flow of terrorist funds and reporting any suspicious activity.

To this end, subject persons who know, suspect or have reasonable grounds to suspect that a transaction may be linked to the FT, whether directly or indirectly, must file a report to the FIAU, as set out under Regulation 15(3) of the PMLFTR. Effective reporting can only be achieved when subject persons adhere to their AML/CFT obligations – by conducting the appropriate level of customer due diligence ('CDD'), ongoing monitoring and transaction monitoring of their customers – since this permits the subject person to become familiar with the customer, make sense of their (expected) activity and detect suspicious activity or known indicators of FT for further scrutiny.

1.1 FUNDING OF TERRORISM IN MALTESE LAW

The offence of FT is defined in Article 328F of the Criminal Code, Chapter 9 of the Laws of Malta, as follows:

> "(1) Whosoever by **any** means, **directly or indirectly, collects, receives, provides or invites** another person to provide, **money or other property** or otherwise **provides finance intending it to be used,** or which he has **reasonable cause to suspect that it may be used,** in full or in part, **for the purposes of terrorist activities** or **knowing that it will contribute towards the activities, whether criminal or otherwise, of any person involved in terrorist activities or of a terrorist group** shall, on conviction, and unless the fact constitutes a more serious offence under any other provision of this Code or of any other law, be liable to the punishment of imprisonment for a term of not less than four years but not exceeding twenty years or to a fine (multa) not exceeding two million and five hundred thousand euro (€2,500,000) or to both such fine and imprisonment.
>
> (2) In this article a reference to the provision of money or other property is a reference to its **being given, lent or otherwise made available**, whether for consideration or not."

The funding of terrorism is thus the process of making funds or other assets available to support, even indirectly, terrorist activities. Indirect support provided to terrorists may take various forms, such as financial compensation, training, propaganda or even assistance related to living expenses. The Criminal Code defines what constitutes an "act of terrorism" and "terrorist activities" in Article 328A.

The process of funding terrorist groups or individual terrorists is addressed in Article 328B and Article 328F of the Criminal Code. The Criminal Code also contemplates other acts that are considered to constitute funding of terrorism. These include the use or possession of money or other property for the purposes of terrorist activities (Article 328G) and the involvement in funding arrangements to support terrorist activities (Article 328H and Article 328I). The criminal offence of funding terrorism under the Criminal Code reflects the definition of funding of terrorism under the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism.

The Criminal Code also treats as criminal offences other acts that are linked to terrorist acts. For instance, Article 328C criminalises:

- receiving or providing training on how to make explosives, weapons or other substances to be used to commit terror activities;
- travelling to or from the EU to carry out, or plan or prepare for terrorist activities or to participate in activities of a terrorist group;
- financing or facilitating travel arrangements for the above; and
- producing, distributing or otherwise making available publications that are likely to encourage or induce the commission of terrorist activities.

1.2 MONEY LAUNDERING VERSUS FUNDING OF TERRORISM

Many of the controls implemented by subject persons serve the dual purpose of combating both money laundering ('ML') as well as FT.

In both offences, there is an attempt or desire to obscure either the source or the destination of funds.

In fact, techniques similar to those employed by money launderers are also often employed by terrorists to:

(i) evade the authorities' attention;
(ii) obscure connections and audit trails; and
(iii) protect the identity of sponsors and beneficiaries of the funds.

Whereas ML is the process of making dirty money appear legitimate, FT attempts to use money which may be either legitimate or illegitimate for the purposes or activities of terrorist groups.

Malta as a financial centre is therefore equally vulnerable to attempts of abuse both by money launderers and terrorist financiers.

Some of the core differences between ML and FT are:

- funds used for ML are derived from criminal activities, while the source of terrorist funds may originate from legitimate and/or illegitimate sources;
- the concealment of funds to be used for terrorism or by terrorists is designed primarily to hide their identity or the purpose for which these funds are used. In ML, the funds are proceeds of illegal activity, and the primary purpose of the laundering is to conceal their source, and enable the funds to be used legally; and
- certain instances of FT may be difficult to detect if funding takes the form of numerous small and potentially insignificant donations, as opposed to large lump sums. Terrorist financiers may employ sophisticated, complex structures, as is the case in large ML operations, but are also known to use low-limit prepaid cards to fund terrorism, despite this being considered a low risk indicator for ML.

ML and FT are separate crimes, and key distinctions exist between the two. Given the urgent nature of CFT, it is essential that subject persons understand these differences and identify signs of FT within suspicious activities.

1.3 HOW DOES FUNDING OF TERRORISM TAKE PLACE?

Although the nature and the number of terrorist groups and threats change over time, the basic necessity for terrorists to raise, move and utilise funds remains the same. International terrorism is dependent on the availability of funds, since funds are utilised for the purchase of terrorist supplies, services, munitions, to finance propaganda and recruitment, travel and education, and to support the families of the deceased fighters.

Terrorism is also dependent on legitimate activities, which are however carried out or connected with terrorists and terrorist groups to generate proceeds, and to win the hearts and minds of their followers. Any material support provided to the legitimate activities carried out by a terrorist or terrorist group strengthens them since it allows them to increase the funds they can dedicate to terrorist activities.

Terrorists or terrorist organisations may obtain funds through:

(i) **licit/legitimate activities**, such as funding through legitimate business activities and charitable contributions or voluntary donations. While the activity itself may be legitimate, e.g. the operation of shops selling goods, this activity is done to support, whether directly or indirectly, terror activities or terrorists themselves, therefore making it a form of FT;
(ii) **misuse of licit activities**, such as the misuse of loans; and
(iii) **criminal or illicit activities**, such as VAT and business fraud, social insurance fraud, counterfeit goods, theft, resale of oil, drug dealing, extortion, hostage taking, human trafficking, credit card fraud, cheque fraud and cybercrime.

Subject persons must be mindful that FT takes place across three main established stages:

(i) the **raising of funds**, which refers to the main sources or activities that terrorists rely on to obtain funding and which may be legitimate (e.g. through charitable donations, business earnings, salaries or small enterprises) or illegitimate (e.g. through ransom, smuggling, sale of stolen goods, including artwork and antiquities, drug trafficking or fuel smuggling);
(ii) the **movement of funds**, which refers to the main channels that are most prone or subject to misuse by terrorists to move funds internationally; and
(iii) the **actual use of funds**, which refers to the location where the terrorist funds are used, either for the terror act itself, in preparation for the terror act (e.g. funds used for propaganda, training or the purchase of airline tickets), or in any other legitimate activity of a terrorist or terror group (e.g. living expenses).

1.4 FUNDING OF TERRORISM IN MALTA

While historically terror attacks have not been common in Malta, terrorism itself and terror financing threats are distinct, and the absence of terror attacks does not mean that Malta is immune to FT. The TF RA carried out by the NCC sought to assess the level of risk of FT to which Malta is exposed, considering both qualitative and quantitative data gathered from a number of sources, including data held by the FIAU, among other authorities. The following sections have been reproduced from the TF RA with the permission of the NCC.

The TF RA was based on a framework that assessed five principal elements:

a) terrorism and FT threats in Malta;
b) FT vulnerabilities at each one of the three stages, namely raising of funds, movement of funds and use of funds; and
c) existing FT controls in Malta.

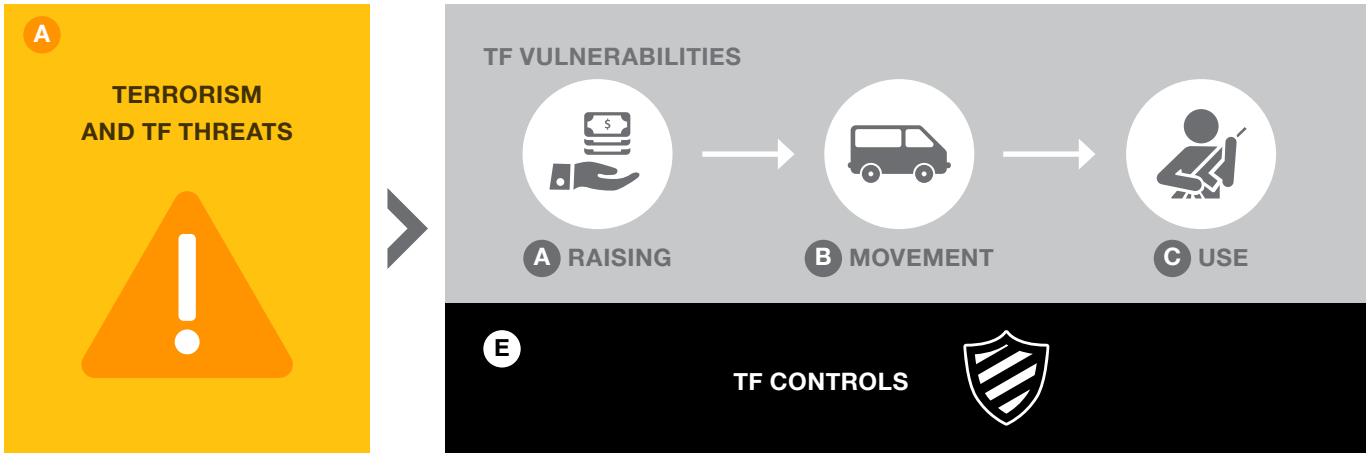


Figure 2 - Image from NCC's TF RA

The TF RA indicated that Malta does potentially face a number of **terror and FT threats** from different types of actors, owing to its geographical position in proximity to countries facing unrest, and to other geopolitical factors.

Likewise, Malta may be vulnerable at any of the three stages, be it the **raising**, **movement** or **use** of funds.

Of course, and as with any other risk assessment, these findings are then subject to an assessment of the legal framework and the **controls** that are in place to mitigate and contain these threats and to address any vulnerabilities.

However, given Malta's open economy and status as an international financial centre, it is most vulnerable to being misused in the **movement of funds** destined for terror activity or terror organisations. The typical demographic and geographical factors associated with financial centres make it unlikely that acts of terrorism actually take place within their borders.

While Malta's proximity to areas of conflict does place it at risk of being used as a transit country for persons transporting physical assets, the more likely exposure to FT for financial centres arises from the high levels of cross-border business, particularly complex transactions, and the international activities of charities and other non-profit organisations (NPOs)[1].

For this reason, this Guidance Document focuses on the typologies and potential means for **facilitating the cross-border movement of funds** though Maltese subject persons.

The TF RA sets out how terrorist actors move funds using a range of channels within and across borders. These channels can be broken down into three categories, with a number of entities and service providers being vulnerable to FT within each category. The TF RA assigned a vulnerability rating in each sector. The following sections set out the three categories and explain the vulnerabilities to which local entities within each category are exposed.

It must be kept in mind that the vulnerabilities identified through the TF RA and replicated below refer to the inherent vulnerabilities; that is, the vulnerabilities that an entity or a sector is exposed to prior to adopting and applying any measures, policies, controls and procedures to mitigate the same. Therefore, the ratings do not take preventive and other mitigating measures into consideration.

1. Monaco Workshop of Financial Centres, Guidance on identifying, assessing and understanding the risk of terrorist financing in financial centres, 2018.

1.4.1 Flow-through

This refers to the possibility that Malta is used as a transit country for funds or other stores of value that may be intended for use in other jurisdictions. Funds flowing through local subject persons typically do not spend much time within Malta, and are swiftly moved again in a process of layering.

1.4.1.1 Credit Institutions

The TF RA identifies the level of inherent vulnerability of credit institutions as 'high'. This is driven by three main factors*:*

- **The size of the sector relative to GDP**: This creates significant opportunity for actors to blend the movement of funds within a high level of legitimate banking activity;
- **The high level of international payment transactions facilitated**: As an international financial centre, Malta processes high levels of payment transactions, many of which pass through credit institutions without any substantive link to the country. It is these transactions that are most likely to be misused by actors wanting to move money across borders; and
- **The number of customers from high-risk jurisdictions**: Information collated as part of the TF RA indicates that Maltese credit institutions serviced a significant number of customers in jurisdictions subject to UN or EU sanctions, or are otherwise considered high risk.

1.4.1.2 Payment institutions, including e-money institutions and other value transfer mechanisms

These institutions enable the transfer of value between persons and across borders. The form that these value transfers can take varies, from money remittance services to internet-based payment and e-money services, and non-internet-based payment services[2].

The TF RA identifies the level of inherent vulnerability of the sector as 'high', primarily driven by two factors related to money remittance services:

- **The high value of remittances overall; and**
- **The high-risk nature of remittances' source and destination.**

Remittance services are particularly important for transferring funds between countries where correspondent banking relations are weak, and are consequently relied on by migrant communities remitting funds to their families in areas with less access to banking services. Remittance services provide a channel to obscure the movement of terrorist funds within a high level of legitimate activity.

Outside certain services that payment institutions provide (i.e. money remittance), the level of exposure of these institutions to FT is moderate.

1.4.1.3 Cash couriers and other cash transfer mechanisms

The TF RA identifies the level of inherent vulnerability of the sector as 'high', driven by:

- **The high level of cash use in Malta**: This provides a significant opportunity to conceal the movement of terrorist funds within a high number of legitimate transactions; and
- **A number of cash smuggling cases and high levels of cash movement into Malta from high-risk jurisdictions**: These incidents have not currently been linked to FT, but are more likely to reflect a lack of awareness of cash declaration thresholds, preference for the use of cash or money laundering. FT exposure nevertheless remains.

1.4.1.4 New and emerging payment technologies

The TF RA indicates that these payment technologies represent a material and growing FT vulnerability, and were assessed as Medium-High. This result was influenced by the actions taken to foster the growth of the virtual financial assets sector, following the enactment of legislation regulating these VFAs. Nevertheless, the TF RA explains that the global prevalence of FT through virtual currencies is relatively low.

With respect to pre-paid cards, the TF RA reveals that the higher risk cards are those that fall within the thresholds, making them eligible for the application of simplified due diligence and which allow cash withdrawals. Locally, the number of these cards in circulation is relatively low, and as such pre-paid cards were not considered to contribute significantly to Malta's risk exposure.

2. The Financial Institutions Act (Cap. 376 of the Laws of Malta) provides a definition of e-money and payment services in its Second and Third Schedules.

1.4.1.5 Other providers of financial services

These include investment services providers and insurance companies, and were assessed as having a Medium-Low inherent vulnerability. While the insurance and securities sectors are large in relation to the size of the local economy, they are unlikely to be misused or abused to facilitate the movement of terrorist funds. As such, it is the size of the sectors relative to the economy that drives the level of exposure.

1.4.1.6 Non-financial legal entities and arrangements

This refers to private limited companies, trusts and foundations. The inherent vulnerability of these entities is assessed as High, driven by:

- the large number of private companies in Malta;
- their complex beneficial ownership structures; and
- the concentration of ownership in foreign individuals.

With that said, the relative lack of FT cases involving trusts and foundations limits the extent of the exposure.

1.4.2 Service providers

This refers to situations where subject persons provide administrative or other services to terror networks, organisations or other entities that support terrorism.

1.4.2.1 Designated non-Financial Business and Professionals (DNFBPs)

Globally, DNFBPs are known to provide services that facilitate FT, particularly to large international terror organisations. The TF RA indicates that DNFBPs represent a Medium inherent vulnerability, which is driven by:

- the large number of TCSPs and legal and accounting professionals in the country (many of which have a significant share of international clientele); and
- the significant growth in Malta's property market, which creates some exposure.

1.4.2.2 Casinos and the Remote Gaming Sector

In Malta, gaming companies represent a Medium-Low FT vulnerability. The vulnerability is mainly driven by the size of the remote gaming sector in Malta, which creates some level of exposure. With that said, the characteristics of owners of gaming licensees and their players suggest that any risk exposure is limited.

1.4.3 Abuse of philanthropic organisations

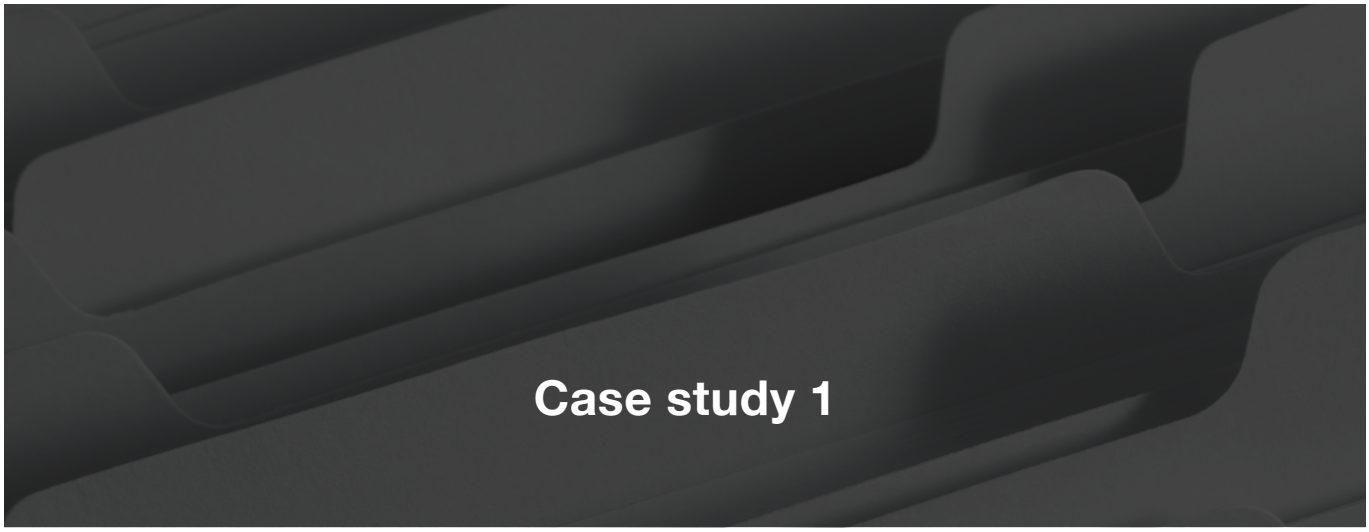
This refers to situations wherein donations or any aid, financial or otherwise, are sent to or administered by subject persons in Malta, and those donations are diverted to support offshore terrorism.

1.4.3.1 Voluntary organisations

These include those trusts, foundations, associations and organisations that are established for a lawful, non-profit making social purpose, and which are voluntary in nature, akin to NPOs. The TF RA assessed the inherent vulnerability of voluntary organisations as being Medium-High. This is driven by:

- **The high number of voluntary organisations**: the majority of local organisations are small, but there are a number that handle larger sums of money. The nature of FT is such that, even small amounts of funds are sufficient to carry out an attack, and therefore even small organisations represent a vulnerability. The high number of organisations increases the exposure; and
- **The fact that a significant number have been designated as high risk from an economic crime perspective**: this risk arises from the nature of activities, countries of operation, as well as size, of a specific number of organisations. This results from an assessment carried out on voluntary organisations.

1.4.4 Local case studies



The movement of terrorist funds using a licensed Maltese Credit Institution

A number of employees working for the same employer held bank accounts with a particular credit institution. The company they worked for was operating within a high-risk jurisdiction, and the industry is internationally recognised as bearing a high ML/FT risk. The bank did not classify the customers as posing a higher risk, and did not monitor them accordingly.

It is only after a while that the credit institution identified a pattern in the transactions undertaken by these customers. They transferred funds back and forth between themselves, labelled as loans and loan repayments. These transfers were significantly high. The bank was not convinced that these loans were legitimate since they did not make any economic or logical sense, and appeared to have been made solely to disguise the audit trail of the funds.

For instance, customer A would transfer a large sum of money to customer B under the appearance of a loan. Subsequently, customer B would then loan Customer C a significant amount of funds, and so on.

The bank conducted more checks on the clients and discovered that their common employer had been identified by reputable media sources to have links with a designated terrorist group.

The credit institution proceeded to report this suspicious activity, which led the FIAU to launch its own analysis.

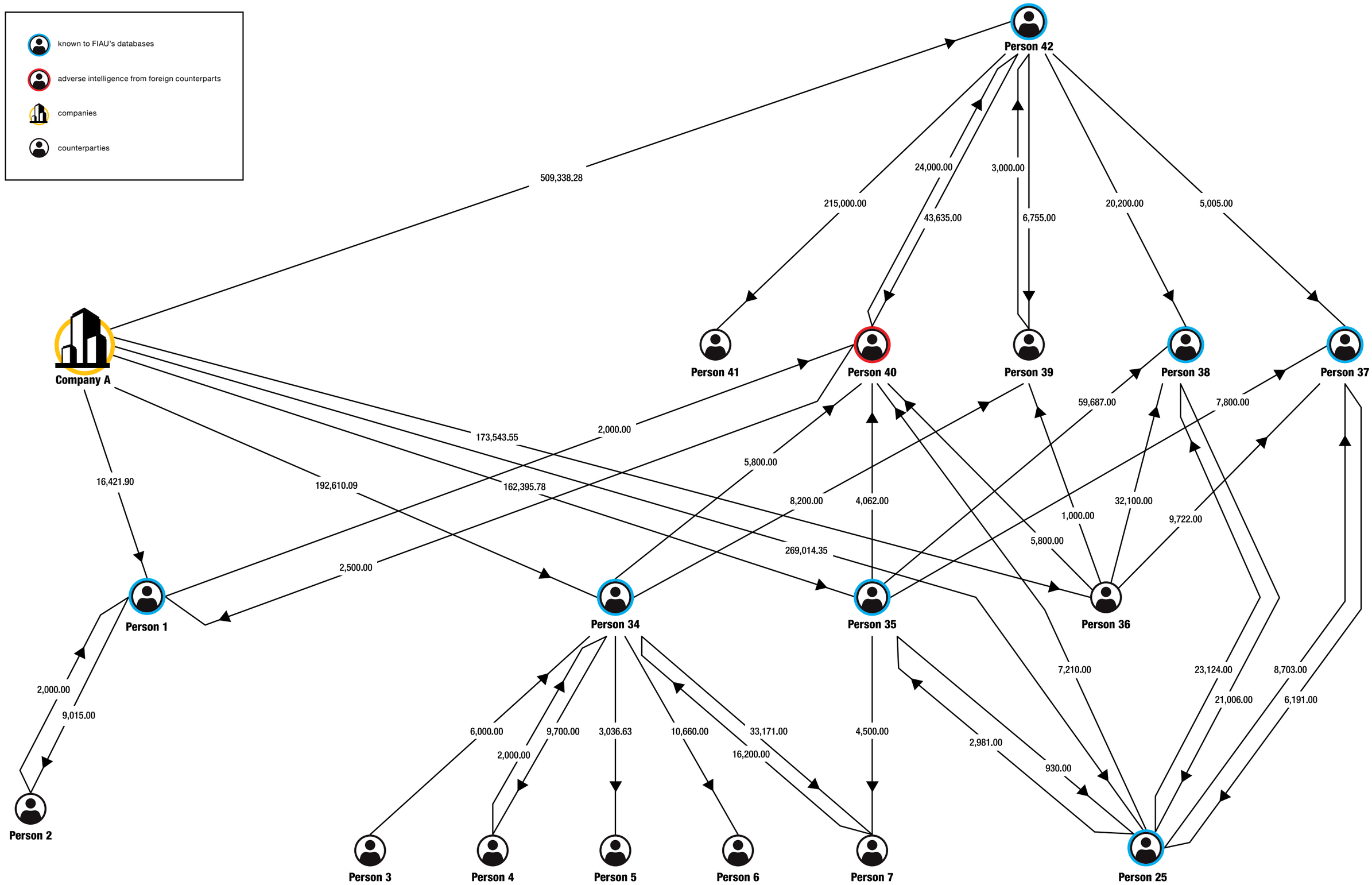


Figure 3 - This diagram represents a cluster that is approximately one fifth of the size of the full web of transactions involved in this case

Case study 2

A Maltese Credit Institution misused to channel funds intended for Terrorism

A foreign counterpart of the FIAU requested information from the FIAU on suspicious activity concerning a crowdfunding company, its Chairman and the Chairman's bank account held with a Maltese credit institution. This led the FIAU to launch an analysis of the suspicious activity and to request information from Maltese credit institutions.

The information gathered by the FIAU revealed that the aforementioned Chairman did in fact hold a bank account with a Maltese credit institution. It was also discovered that the person ran a charity that received and donated funds to multiple charitable causes and jurisdictions that required humanitarian aid. Further analysis established that the person belonged to an extremist Islamic movement, and that the charity, which he presided over, was linked to other non-profit organisations that supported radical Islamic causes.

The analysis also identified significant inward payments that were made in favour of the Chairman's account, held with the Maltese credit institution. These transactions originated from the crowdfunding company, for onward remittance to various individuals. The first transaction involved an EU company that deposited €90,000 into the Chairman's account, following which the Chairman transferred money from his accounts in smaller, fragmented amounts, ranging from a few hundreds to a few thousands, in favour of numerous persons, mainly bearing other EU IBANs.

On one particular day, the Chairman received a payment of €150,000 from a PayPal account, and proceeded to send out a total of €88,813 in favour of another natural person through six structured transactions. Transactions from the Chairman's bank account also indicated that he remitted close to circa €600 to a person who is suspected by the Malta Police Force to be a terrorist.

It is worth pointing out that, while this data and information was available to the Maltese credit institution in question, the subject person did not report this suspicious activity on its own initiative, but rather did so after being probed following the FIAU's request for information.

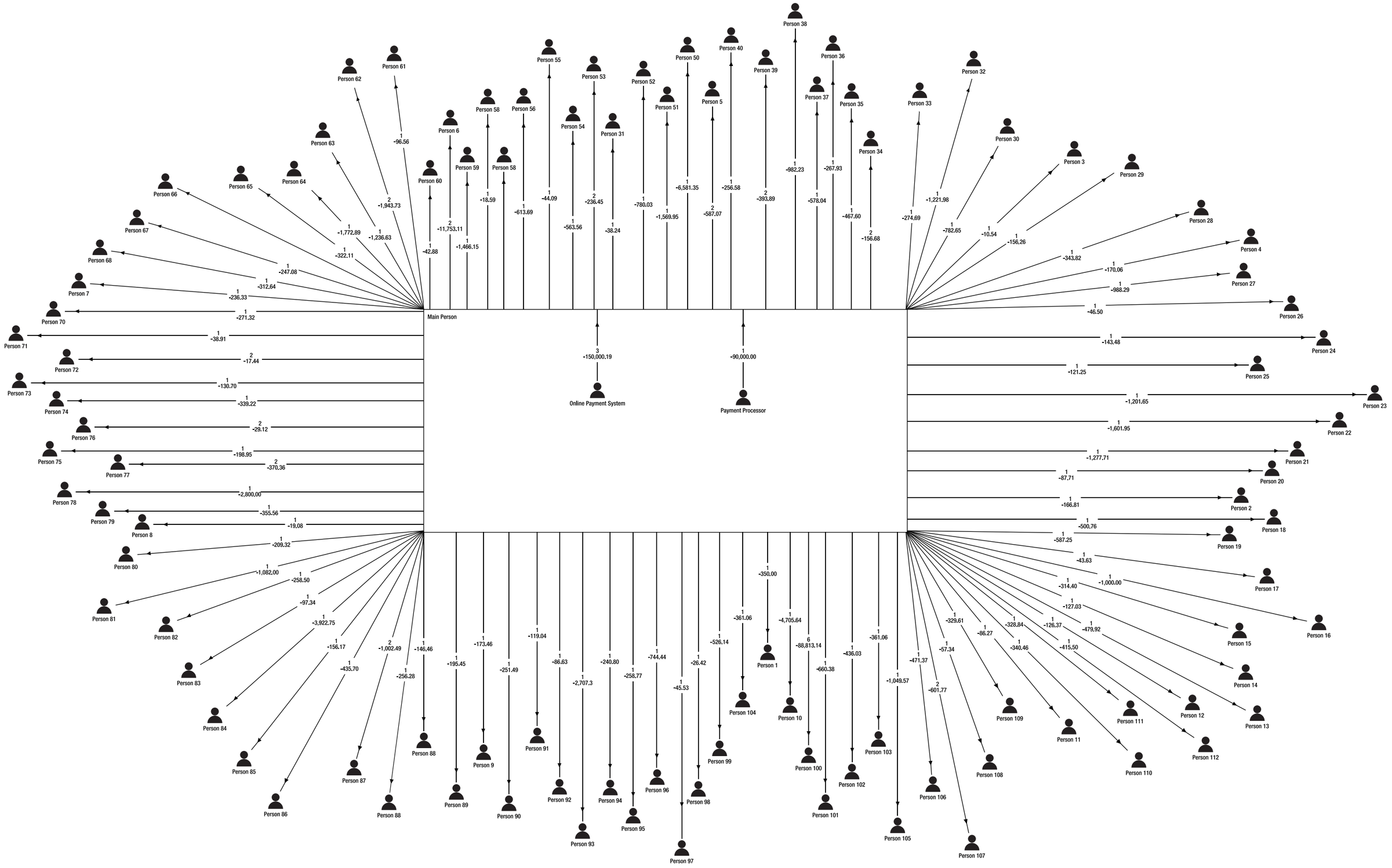

Main Person
Online Payment System
Payment Processor
Person 1
Person 2
Person 3
Person 4
Person 5
Person 6
Person 7
Person 8
Person 9
Person 10
Person 11
Person 12
Person 13
Person 14
Person 15
Person 16
Person 17
Person 18
Person 19
Person 20
Person 21
Person 22
Person 23
Person 24
Person 25
Person 26
Person 27
Person 28
Person 29
Person 30
Person 31
Person 32
Person 33
Person 34
Person 35
Person 36
Person 37
Person 38
Person 39
Person 40
Person 50
Person 51
Person 52
Person 53
Person 54
Person 55
Person 56
Person 58
Person 58
Person 59
Person 60
Person 61
Person 62
Person 63
Person 64
Person 65
Person 66
Person 67
Person 68
Person 70
Person 71
Person 72
Person 73
Person 74
Person 75
Person 76
Person 77
Person 78
Person 79
Person 80
Person 81
Person 82
Person 83
Person 84
Person 85
Person 86
Person 87
Person 88
Person 88
Person 89
Person 90
Person 91
Person 92
Person 93
Person 94
Person 95
Person 96
Person 97
Person 98
Person 99
Person 100
Person 101
Person 102
Person 103
Person 104
Person 105
Person 106
Person 107
Person 108
Person 109
Person 110
Person 111
Person 112
1 -42.88
2 -1,943.73
1 -96.56
2 -11,753.11
1 -1,466.15
1 -18.59
1 -613.69
1 -44.09
1 -563.56
2 -236.45
1 -38.24
1 -780.03
1 -1,569.95
1 -6,581.35
2 -587.07
1 -256.58
2 -393.89
1 -982.23
1 -578.04
1 -267.93
1 -467.60
2 -156.68
1 -274.69
1 -1,221.98
1 -782.65
1 -10.54
1 -156.26
1 -343.82
1 -170.06
1 -988.29
1 -46.50
1 -143.48
1 -121.25
1 -1,201.65
1 -1,601.95
1 -1,277.71
1 -87.71
1 -166.81
1 -500.76
1 -587.25
1 -43.63
1 -1,000.00
1 -314.40
1 -127.03
1 -479.92
1 -126.37
1 -328.84
1 -340.46
1 -86.27
1 -415.50
1 -329.61
1 -57.34
2 -601.77
1 -471.37
1 -1,049.57
1 -361.06
1 -436.03
1 -660.38
6 -88,813.14
1 -4,705.64
1 -350.00
1 -361.06
1 -526.14
1 -26.42
1 -45.53
1 -744.44
1 -258.77
1 -240.80
1 -2,707.3
1 -86.63
1 -119.04
1 -251.49
1 -173.46
1 -195.45
1 -146.46
1 -256.28
2 -1,002.49
1 -435.70
1 -156.17
1 -3,922.75
1 -97.34
1 -258.50
1 -1,082.00
1 -209.32
1 -19.08
1 -355.56
1 -2,800.00
2 -370.36
1 -198.95
2 -29.12
1 -339.22
1 -130.70
2 -17.44
1 -38.91
1 -270.32
1 -236.33
1 -312.64
1 -247.08
1 -322.11
1 -1,772.89
1 -1,236.63
3 -150,000.19
1 -90,000.00

Figure 4

Case study 3

A web of suspicious activity detected by a Maltese Credit Institution

A Maltese credit institution noted existing similarities and suspicious activity linked to FT in a number of its customers, mainly persons from the African region, and proceeded to submit a total of 46 STRs to the FIAU. The similarities related to the individuals' employment, transactional activity, residential addresses and flight ticket purchases – all of which revealed several links and relationships between the individuals.

The STRs submitted led the FIAU to launch a financial analysis on a total of 58 individuals. These persons were suspected of being involved in human smuggling/illegal immigration, as well as the funding of terrorism, by providing financial support, particularly relating to logistical expenses, to individuals linked with terrorist organisations and their sympathisers. For example, one of these individuals was later arrested in an EU country following suspicion that the person was aiding illegal immigration and of assisting persons involved in terrorist organisations.

On analysing the customers' transactional activity, various trends and commonalities were identified. All the customers purchased a considerable number of airline tickets, both for themselves and for third parties. In fact, a total of 4,418 airline ticket purchases were identified, of which 600 were conducted by the same individual who was later arrested due to his links with a terrorist organisation recruiter and his involvement in a migrant trafficking ring.

Furthermore, it was also noted that their bank accounts were funded by frequent cash deposits, as well as considerable amounts of third-party cheque deposits. The customers also conducted a number of remittances towards third parties in foreign jurisdictions and a high number of Voice Over IP subscription purchases were also noted.

The hereunder sanitised chart demonstrates the relationships and common links between the individuals concerned, which could indicate that these persons may be involved in a common organisational framework.

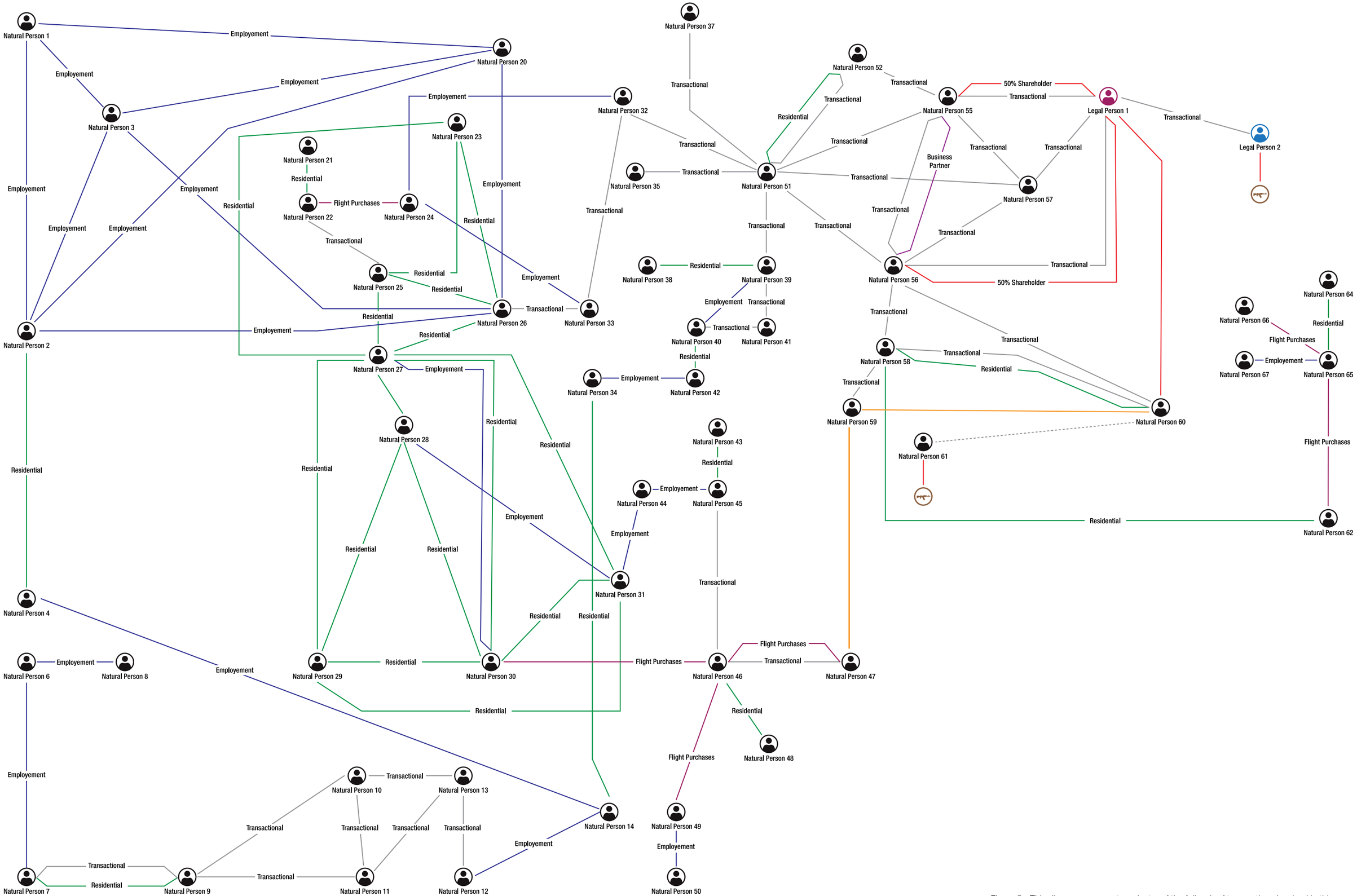


Figure 5 - This diagram represents a cluster of the full web of transactions involved in this case

2. TYPOLOGIES AND EMERGING TRENDS IN FT

This section describes some of the better known methods and emerging trends in FT, including indicators of suspicion (red flags) associated with this phenomenon. The adaptability and opportunism shown by terrorist organisations suggests that all the methods that exist to move money around the globe are to some extent at risk. It must be borne in mind that no single red flag is a clear indication that FT is or may be taking place.

The occurrence of any indicators has to be considered holistically and on a case-by-case basis within the context of the services and products being offered, as well as based on what is known about the customers, including on their declared activity, their source of funds and the possible reasons behind a particular transaction. After an assessment has been carried out, the subject person will be in a better position to determine whether they have the required knowledge, suspicion or reasonable grounds to suspect that FT is or may be taking place. An STR must be submitted immediately with the FIAU when this is the case.

Subject persons should refer to Section 8.1 of the Implementing Procedures Part I on Introducing the Concepts of Non-Reputable Jurisdictions and High-Risk Jurisdictions for guidance on assessing the risks of a jurisdiction, being mindful of those jurisdictions within which terrorism is active, as well as those jurisdictions having strong communal links to areas with an active terrorist threat.

2.1 CASH

2.1.1 Vulnerabilities

Physical coins and bank notes may be used for FT purposes in a number of ways. Cash may be used as a means of payment, or deposited into accounts held with credit and financial institutions. It may also be used to purchase value instruments, such as pre-paid cards.

Cash may be indicative of funds being moved via cash couriers or postal services. It is one of the most commonly identified modus operandi among terrorist organisations for moving funds for a number of reasons:

(i) it may be used anonymously;
(ii) it is difficult to trace;
(iii) it may be transported across borders undetected;
(iv) it leaves no audit trail from one person to the next; and
(v) it is one of the most common and traditional payment methods in the black market. In fact, cash may be the most frequently used payment method in the areas where terrorist organisations operate.

2.1.2 Red flags

- The use of larger cash denominations, since persons transporting cash find it easier to move cash in smaller bulks, and therefore, may opt to exchange the accumulated funds (which would usually be made up of smaller denominations), into larger denominations that are internationally accepted (such as €100, €200 or €500 notes).
- Bulk cash withdrawals or the possession of cash coinciding with travel arrangements to areas where terrorist groups are active, or in close proximity thereto, or to areas where terrorist groups are known to enjoy support, or cash withdrawals from those countries.
- Cash withdrawals from Automatic Teller Machines ('ATMs') in high-risk countries, or those in close proximity thereto, especially but not exclusively following the receipt of incoming transfers.
- Patterns of large (i.e., close to the maximum withdrawal limit), repetitive, round-sum cash withdrawals from different ATMs in high-risk countries or those in close proximity thereto.
- The use of substantial amounts of cash to purchase or lease high-value goods, such as immoveable property or yachts, especially when this activity is undertaken by persons from high-risk jurisdictions, since the true source of these funds may be difficult to ascertain. This risk is particularly relevant given the high volumes of cash brought in from high-risk jurisdictions.
- Requests for payment to be made in cash for the purchase of high-value goods since terrorists are known to use cash to move funds.

2.2 FUND TRANSFERS AND MONEY REMITTANCE

2.2.1 Vulnerabilities

Funds may be transferred through the formal financial system, i.e., through legitimate and regulated credit and financial institutions, but also informally through unregulated systems, known as Informal Value Transfer Systems ('IVTSs').

Unregulated systems

IVTSs are attractive for terrorist financiers since these provide them with an opportunity to move funds around under the radar.

One of the most popular methods of an IVTS is Hawala, also referred to as hundi, poey kaun, chop shop banking and chiti banking. Hawala is used to transfer funds across borders in a relatively safe and convenient manner, involving people in various parts of the world who use their accounts to move money internationally for third parties. Hawala banking involves informal financial service providers, who carry out financial transactions whereby cash, valuable goods and cheques are accepted at one location and a corresponding sum of equivalent remuneration is paid at another location.

IVTSs are attractive to terrorist financiers and a popular means of transferring funds, particularly because they operate under the supervisory radar and do not comply with regulatory requirements to keep detailed records or to submit reports. Particularly in the case of Hawala banking for instance, the international money audit trail is completely eliminated, since funds do not actually cross borders.

The trend is for the money transfer to be completed by coded information (such as an identifiable number) passed through various portals of choice, such as letters, on-line chat systems, e-mails and text messages. Nowadays, Hawalas and similar agents have moved away from using traditional methods of communication to using advanced, protected internet technologies, since this shift eliminates manual accounts and record-keeping evidence. This is then followed by a telecommunications confirmation, which discloses an identifiable number to be used by the receiver to pick up the values in the other country.

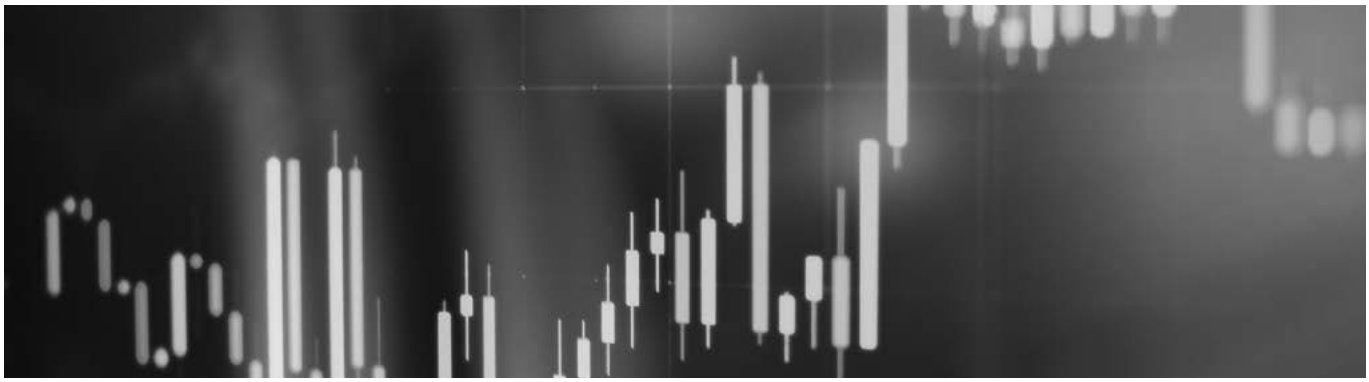
The reason why Hawalas and other IVTSs are difficult to identify is because the persons involved in this process tend to operate within or in addition to a front or legitimate business to provide cover for the activity and to co-mingle funds in business accounts.

Case study 4

Hawala banking used to move funds destined for terrorist groups

Hawala money was provided by country A's terrorist organisation leaders and routed through country B, where another of the terrorist organisation's workers was located, in the following manner:

(i) The terrorist leader in country A collects terror funds in that country and sends it to another terrorist agent in country B;
(ii) This agent contracts a hawaladar, who operates freely in that country;
(iii) The hawaladar in country B gives a number to the agent on a currency note, along with the telephone number of the person who would deliver the money;
(iv) The agent then passes on this information to country A's terrorist leader;
(v) Country A's terrorist leader then contacts country B's worker and forwards the hawaladar's telephone number and the number indicated on the currency note;
(vi) The worker then contacts the hawaladar at the given number and collects the money at the determined location after giving the number of the currency note. The worker would not get to know the identity of the hawaladar since he delivers the funds wearing a scooter helmet.



Regulated/Formal Systems

Owing to the veil of legitimacy that licensed institutions provide, and especially owing to the necessity of having bank accounts to carry out day-to-day activities (e.g., to deposit one's salary or social benefits and to make on-line payments), regulated credit and financial institutions remain a prominent channel for fund transfers intended to support terrorists.

Therefore, even individuals who use IVTSs are likely to be customers of regulated institutions, using their products or services to inject the tainted funds in the financial system. 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.

Credit and financial institutions run the risk of being misused in any of the three stages of FT described in Section 1.3 above; that is, in the raising, movement or actual use of funds. Owing to their prime position in detecting suspicious transactions and suspicious activity, it is imperative for them to understand emerging trends in FT and implement effective, ongoing monitoring. This is especially necessary since some of the most commonly detected FT typologies are connected to the products or services offered by credit and financial institutions. These include the structuring of deposits to, or withdrawals from, bank accounts; the purchase of money instruments (including bank cheques and money orders); the use of bank cards; and fund transfers.

Case study 5

Financial indicators following a terrorist attack

A customer held two bank accounts with two licensed institutions. A day before a terrorist attack, the customer structured a number of cash withdrawals from different ATMs to avoid detection.

Later, the terrorist attempted to purchase flight tickets to high-risk jurisdictions using two credit cards, but the transactions were declined by both cards since the amount was in excess of the cards' credit limit. Thus, the terrorist proceeded and succeeded to purchase different and cheaper flights.

The terrorist then completed a bank transfer, and attempted another two transfers, of over €1,000 to a local charity that had potential links to terrorism. The person also made other transactions to purchase jewellery, designer clothing and escort services. Various other purchases were attempted and declined because these were in excess of the cards' credit limit. It also emerged that various purchases were made by the terrorist for firearms.

2.2.2 Red flags

- Fund transfers that are seemingly without any legitimate or reasonable explanation to or from areas where terrorist groups are active, or in close proximity thereto, or to areas where terrorist groups are known to enjoy support.
- Transfers of funds to the same beneficiary account but with the recipient indicated with different names.
- Payments related to the acquisition of substances and materials that are not related to, or in quantities that are unusual for, the individual's known activities and can be used in the construction of explosive devices (e.g., the acquisition of aluminium pipes, shooting equipment, fertiliser and scrap iron).
- Payments related to travel arrangements to or from areas where terrorist groups are active, or in close proximity thereto, or to areas where terrorist groups are known to enjoy support or payments made in relation to communication services provided in these areas.
- The customer's transaction activity does not tally with his/her profile.
- Salary accounts that are used to purchase airline tickets to higher risk jurisdictions or those in close proximity thereto, and subsequently the bank account becomes dormant or inactive for a period of time thereafter.
- Active bank account goes dormant for a few months and subsequently becomes active again, particularly if it becomes intensively used. This is especially alarming if this dormancy coincides with the purchase of flight tickets or travel arrangements.
- The creation and use of multiple accounts without any legitimate or economic reason.
- Bank account activity conducted remotely (e.g., through on-line banking, ATMs, debit/credit cards, etc.) from areas where terrorist groups are active, or in close proximity thereto, or to areas where terrorist groups are known to enjoy support. Particular vigilance should be exercised when this remote access coincides with the receipt or transfer of significant sums of money or if this follows a period of prolonged account inactivity.
- Transactions that contain terms or references, e.g., in the SWIFT, which may be in a foreign language and which may be associated with extremist beliefs, terrorist ideologies or short, suspicious messages, such as mujahid/mujaheed/mujahideen (the term for someone in Jihad) and ghanimah/fai/fay (justified stolen funds).
- References to Zakat/Zakah, Jizyah, Ghanimah, Khums and Saleb, although not of themselves harmful, may be indicative of FT when accompanied with other high-risk factors, such as remittance to higher risk jurisdictions.
- Fund transfers involving indications of wire stripping, which is the deliberate act of changing or removing information from payments or instructions, thus making it difficult to identify and restrict transactions to and from sanctioned individuals, entities or jurisdictions.
- Lack of documentation and/or vague justifications when questioned on fund transfers to high-risk jurisdictions or entities.
- The customer makes unusually large cash withdrawals, especially if this is done after the financial institution refuses an overseas fund transfer (therefore raising suspicion on cross-border cash smuggling).
- Fund transfers to or from entities that are subject to international or EU sanctions.
- Fund transfers to or from entities that, though not subject to any international or EU sanctions, are known to be sympathetic to, or have links with, terrorist groups.
- Fund transfers to or from individuals and/or entities involved in the informal financial sector (e.g., Hawala).
- Fund transfers to legal businesses or companies that might not make economical or logical sense. These entities may be cover structures and may be used to assist them in the receipt, movement and eventual use of funds.
- Fund transfers made to accounts outside the country that have a fundraising purpose; while not necessarily indicative of FT, these transfers should be scrutinised.
- The customer uses money remitters to transfer funds to high-risk jurisdictions, or redeems funds from them, which funds may either be significant, or the customer does not seem to have any apparent established links with the said jurisdiction or does not provide any founded explanations (such as familial ties).
- The customer cashes bank drafts in foreign currencies before travelling to high-risk countries, or makes use of travellers' cheques or pre-paid cards in areas where terrorist groups are active, or in close proximity thereto, or to areas where terrorist groups are known to enjoy support. Vigilance should also be exercised in the case of open-loop cards used to withdraw funds from ATMs in these jurisdictions.

2.3 VIRTUAL FINANCIAL ASSETS

2.3.1 Vulnerabilities

To be read in conjunction with Section 2.5 of Annex 1 of the Implementing Procedures – Part II for the Virtual Financial Assets Sector.

Virtual Financial Assets ('VFAs') may be misused for FT purposes since they are a powerful tool for terrorist financiers to move and store illicit funds.

There are various manners through which funds are raised or moved via VFAs. VFA exchanges may be used to transfer and/or exchange funds from FIAT currency to VFAs, and utilise the VFAs as a means of payment within black markets, or on the Darknet for the purchase of illicit material. VFAs may also be withdrawn in cash from crypto-ATMs, or exchanged to FIAT currency and subsequently withdrawn, which funds are used for or to support terror activities.

There are also known instances of ransomware attacks, when hostages or victims are forced to make payments in VFAs to specific wallet addresses to regain access to their data. Another emerging trend used by terrorists to fund their activities is to solicit donations in VFAs from sympathisers.

Originally, the tendency was for terrorist groups to request that funds be sent to a single digital address or wallet. However, in a bid to ensure that donations remain anonymous and to render it even more difficult for law enforcement agencies to track and/or trace them, the trend has evolved in that each donor is being assigned a unique address through which to send the digital currency.

VFAs may be attractive for terrorist financiers because:

- they have been designed to be decentralised, and thus may not always be subject to supervision and oversight by a licenced institution;
- convertible virtual currencies can be exchanged for FIAT or other virtual currencies that would then be used as a funding method;
- users can receive payments from unknown sources from any jurisdiction;
- they are more anonymous than traditional, non-cash payment methods since they may be used by anyone with access to the internet anywhere in the world without the oversight of a centralised authority;
- transactions are usually non-face-to-face;
- there is the possibility of anonymous funding, whereby the funding source may remain obscure;
- if the sender and the recipient are not identified or not identified properly, anonymous transfers can easily take place;
- they are generally the payment method that is accepted by vendors on the dark web;
- privacy coins may completely obfuscate the financial audit trail;
- mixers or tumblers may be used to obscure the financial audit of the VFAs;
- certain digital wallets, which enable data anonymisation, may be used and, as a result, render VFA payments even more untraceable;
- illicitly tainted or illegally obtained VFAs may be deposited into crypto-linked credit cards to give an apparent licit means of payment. Illicit physical cash may also be deposited to these cards via ATMs;
- VFA prepaid cards may be used, which allow users to load the card with VFAs and use as payment methods anywhere where major cards are accepted;
- certain VFAs, like Bitcoin, may also be purchased from crypto-ATMs with physical cash, whereby the VFAs may then be stored on a bitcoin address or wallet, which could be non-custodial, thereby bypassing the requirement of KYC; and
- VFAs may be purchased and transferred peer-to-peer, thereby bypassing AML/CFT obligations, such as the FATF's travel rule.

2.3.2 Red flags

To be read in conjunction with Chapter 1 of Annex 1 of the Implementing Procedures – Part II for the Virtual Financial Assets Sector.

- The customer uses an anonymised method of payment, including privacy coins such as DASH and Monero, since these protect the identity and ensure the anonymity of users of these coins. Privacy coins have features that allow for the obfuscation of the address of the sender, the receiver and the amount sent, significantly increasing anonymity, and thus the risk that they may be used for illicit activities and ML/FT.
- The customer uses mixers or tumblers that obscure the financial audit of the virtual assets.
- The customer uses certain digital wallets that enable data anonymisation by obfuscating crypto transactions carried out on-line by allowing illicit transactions to digitally piggyback on legitimate transactions, rendering VFA payments even more untraceable, such as DarkWallet and Bitcoin Fog.
- The customer's account is funded with funds held with institutions located in high-risk jurisdictions.
- The transaction's script and/or payment narrative suggests an illicit activity.
- The customer makes transactions to wallets or addresses tainted with suspicious or illicit activity.
- The customer uses or transfers VFAs to areas where terrorist groups are active, or in close proximity thereto, or to areas where terrorist groups are known to enjoy support.
- The customer receives frequent or large value deposits, or deposits adding up to significant amounts, of VFAs through crypto-ATMs located in high-risk jurisdictions or from areas known for their high rate of criminal activity.
- The customer uses credit or debit cards that store VFAs, may be debited with VFAs and whose value is withdrawn from ATMs or crypto-ATMs within high-risk countries or jurisdictions in close proximity thereto. This is a prominent red flag since certain designated terror groups are known to make use of this activity.

Case study 6

Raising funds for terrorist organisations using VFAs

Users of an encrypted call and messaging application post the web links of a website known to contain ISIS propaganda and content, and solicit other users to donate cryptocurrency to the website through a wallet address.

Two weeks later, a reader replies that, through this fundraising activity, computers for jihadis had been purchased.

2.4 LOANS

2.4.1 Vulnerabilities

A prominent emerging trend is the misapplication of loans, whether payday loans, microloans, personal loans, vehicle loans or student loans. Small and short-term loans are increasingly becoming attractive for terrorist financiers, wherein multiple applications for loans would be made to various providers simultaneously with no intention to repay the loaned funds. When loans are obtained fraudulently, more often than not the loaned funds would not be intended to be used for the purpose for which the loan was granted. When the funds are given directly to the customer as opposed to the supplier of the product or service, there is a higher risk that the loaned funds may be misused.

Case study 7

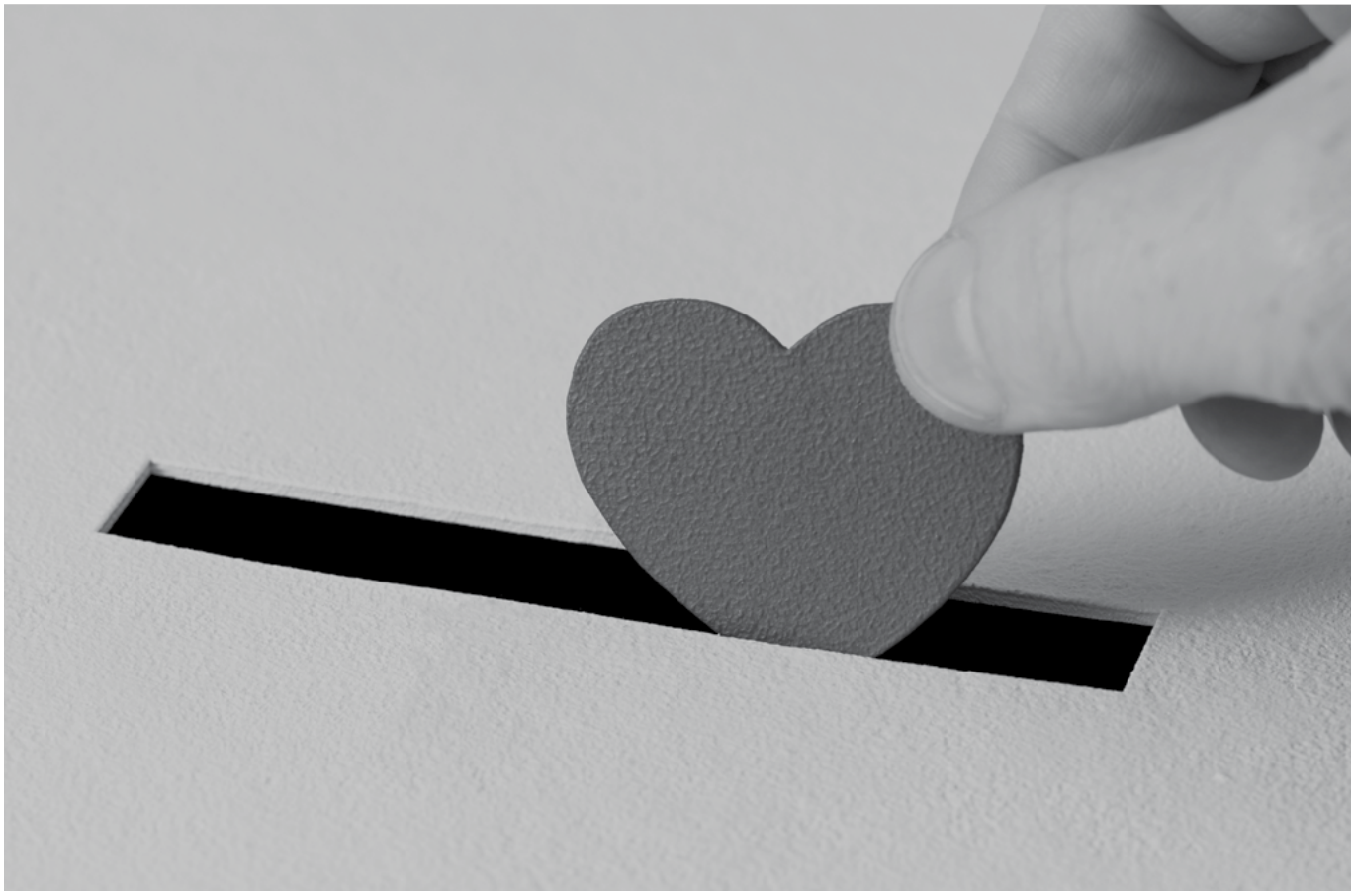
Student loan misused for FT

A teenager from the United Kingdom, who was later identified as being a terrorist sympathiser, used a forged certificate from an educational institution to apply for tuition at a university, for which he received student loans and educational grants. The funding obtained through these loans was used to purchase five flights, for himself and four friends to Morocco; after which, the five individuals proceeded to fly to separate destinations within Turkey.

His four friends successfully crossed the border into Syria to join the Islamic State. However, the teenager had a change of heart and returned to Istanbul instead, where he was arrested by British police at the British consulate. He was subsequently sentenced for terrorism offences, including engaging in conduct in preparation for committing an act of terrorism, and engaging in conduct with the intention of assisting others to commit acts of terrorism, as well as for fraud by deception.

2.4.2 Red Flags

- Forged or falsified documentation or payslips.
- Delaying tactics or reluctance to provide the requested CDD documentation.
- Customers with low income or on social benefits apply for loans that are not in line with their profile.
- Purpose of the loan does not coincide with the information known about the customer.
- The customer does not provide documentation as evidence that the loan was used for the purpose it was granted.
- Defaulting on loan repayments. In the case of vehicle loans, this is particularly alarming when it comes to your attention that the customer has reported the vehicle as stolen to claim insurance.
- Multiple loan applications to various institutions or loan providers in a short period of time.
- Multiple customers seeking the services of the same subject person who provide documentation authenticated by the same certifier and/or have a similar employment status and request similar loan amounts, indicative of persons working in groups or for the same organisation.
- The customer carries out various and/or significant cash withdrawals, or purchases airline tickets immediately after having been granted a loan.



2.5 NON-PROFIT ORGANISATIONS AND CHARITIES

2.5.1 Vulnerabilities

Purpose foundations and voluntary organisations, including charities, are attractive to terrorists and vulnerable to misuse for FT because they enjoy public trust, have access to funds and their activities are often cash intensive. Charities are more susceptible to misuse since they are usually subject to lighter regulatory requirements, as opposed to other financial institutions or corporate entities.

Some charities also have a global presence, thereby providing a framework for national and international operations and financial transactions. The highest risk lies with those purpose foundations and voluntary organisations that operate in or near areas that are exposed to terrorist activity and that receive funds from or distribute funds to these countries. Subject persons should pay close attention to donations made to:

- purpose foundations or voluntary organisations having connections with geographical areas that are high risk, ungoverned, known to have poor AML/CFT oversight, or where terrorists are active or operate in close proximity;
- purpose foundations or voluntary organisations having connections with geographical areas that are under-developed or where the welfare available from the state is limited or non-existent; and
- purpose foundations or voluntary organisations that are known or suspected to have been infiltrated by terrorists.

The trend is for funds to be pooled from numerous small donors. These funds are then sent overseas to troubled locations in the world under the disguise of a charity, thereby providing a veil of legitimacy. This is an attempt by the fund-raising operation to avoid raising alarm bells, since it would appear as an ordinary charity transferring funds to unsettled jurisdictions.

There are three typical scenarios that demonstrate how charities may be abused or exploited. Each of these scenarios has certain characteristics indicative of FT:

(i) **Diversion of funds or fraud within legitimate charities**, where persons donate money to charities that are set up for legitimate charitable purposes. The funds are transferred to the place of need by the charity, but rather than going to the intended charitable projects or purposes, the funds are 'hijacked' and diverted by ill-intended persons to fund terror activities.

Case study 8

Exploitation of a legitimate charity

Suspicious activity was reported by a credit institution following an attempt by an individual to deposit large amounts of cash into a charity's account, with the instruction that these funds be transferred to a notary as an advance for the purchase of real estate. This individual had a power of attorney of the said charity.

Payments into the charity's account consisted of multiple cash deposits, which the credit institution presumed to be donations, and transfers were also made from the individual's personal account to that of the charity's. This person's personal account also had a record of multiple cash deposits and transfers from various individuals.

The person's account also revealed numerous international transfers made to individuals known for terrorist activities. It eventually materialised that the charity, which was a legitimate one, was being exploited by this individual. It was being used as a front to raise funds and to divert a portion of the charity's funds and other funds to terrorists.

(ii) **The use of a sham organisation that poses as a legitimate charity** as a front organisation for a terror organisation or terror groups. In such cases, financial institutions and other persons or entities providing services to the organisation – such as its establishment and registration, payment accounts and fund transfers, as well as accounting services – would unknowingly be providing their services to terror financiers and/or terror networks. Likewise, funding could be provided by persons making monetary donations to what they believe to be a legitimate charitable cause. The funds would then be distributed for use by terrorists.

Case study 9

A pretence charity

A credit institution submitted an STR on a non-profit organisation with a branch in Russia because of a discrepancy between the stated objectives of the organisation and its actual expenditure.

It transpired that funds were being transferred from the organisation to shell or fictitious entities, which funds would then be withdrawn and/or forwarded to militants.

(iii) Broad **exploitation**, where charitable organisations, such as purpose foundations or voluntary organisations, intentionally raise funds for persons in a third country who form part of or support a terrorist organisation.

Case study 10

Misuse of charities

A charity in the United States of America often held fund-raising events. Annually, it would transfer millions of dollars overseas, most commonly to strife-torn regions, such as Kashmir, Bosnia, Afghanistan, Chechnya and Lebanon.

It later transpired that there were two types of donors: those who believed they were giving money for humanitarian relief; and those who were aware of the purpose of their donations. Some of the latter even included terrorism-supporting statements in the transaction reference.

The funds raised would be transferred to an overseas office of the charity or to an affiliated charity, after which the funds would be diverted to terrorist facilitators in the overseas territory.

Case study 11

Allegations of a charity and its trustee being linked to terrorist groups

A Charity Commission investigated a registered charity delivering aid and relief to a group of persons around the world, but particularly in high-risk jurisdictions, after allegations that it was an integral part of a designated terrorist organisation and that one of the charity's trustees had links to terrorist organisations. During its investigation, the Charity Commission sought to understand whether the charity was supporting the ideology or activities of the said terrorist organisations.

The Charity Commission concluded that the charity was not funding or supporting groups supporting terrorism. However, it also ordered ample improvements in procedures for the selection of local charity partners in high-risk territories, as well as procedures for overseeing their activities owing to the allegations made that one of the charity's trustees had links to terrorist organisations. Additionally, it ordered the charity to completely disassociate itself from a particular organisation known to channel money to and support terrorist organisations.

2.5.2 Red Flags

- The use of funds by the non-profit organisation is not consistent with the purpose for which it was set up.
- Inconsistencies arise between the size or pattern of the financial transactions of the non-profit organisation and the stated purpose or activity of the same.
- The customer or the agent frequently deposits funds in the account held by the charity, which charity is located in or transfers funds to high-risk jurisdictions, or has been identified to have possible links to FT.
- Any of the parties to the transaction (account owner, recipient, beneficiary or the sender) has links with conflict areas or jurisdictions that have been identified as supporting terrorist activities.
- The customer or the agent co-mingles their personal funds or their business funds with that of the charity, whether by transferring or depositing these funds to the account held by the charity.
- The customer or the agent's personal account demonstrates gambling activity that coincides with withdrawals or fund transfers from the charity's account (with, for example, utility references).
- The customer or the agent withdraws or transfers funds from the charity's account and deposits these into their own account, and later conducts outward transfers from their own account to that of a third party.
- Adverse media reports on the charity linking it to terrorist activities.
- When fundraising events have been held, a third party is then authorised to be a signatory to the charity's accounts, and the third party then uses this to transfer funds to high-risk jurisdictions.
- Transactions carried out by the charity, which include suspicious terms or terms known to be linked to terrorism in the transaction description.
- Fund transfers made by the charity to another charity or donor, since this may be a tactic being employed to move funds and disrupt the audit trail, and may be indicative of the charity being a cover structure.
- A lack of documentation and weak justifications when questioned on its activities or any transfers carried out.
- The non-profit organisation has little or no staff, which is suspicious considering its stated purpose and expected financial activity.

Not all funds sent overseas are automatically indicative of a suspicion of ML/FT. When relief is sent to areas of conflict or high-risk jurisdictions, subject persons must ensure that the appropriate level of CDD is conducted, particularly in relation to the beneficiaries. Subject persons must assess all the circumstances and available information to determine whether they suspect FT, and, if so, report any suspicious activity immediately to the FIAU.

2.6 LEGAL PERSONS AND ARRANGEMENTS

2.6.1 Vulnerabilities

Legal persons and arrangements are vulnerable to FT particularly in the first two stages – the raising and movement of funds:

(i) in the first stage, which is that of the raising of terrorist funds, the funds of legitimate businesses may be used to support terrorist activities or organisations, particularly in those industries that do not require formal qualifications to operate and those businesses that do not require significant investments to start operating. Moreover, the risk that funds derived from a business will be diverted to support terrorist activity is greater in those businesses where the sales reported and the actual sales carried out are difficult to verify, as is the case with cash-intensive businesses; and

(ii) in the second stage, which is that of the movement of funds, legal persons and arrangements, including complex structures and structures set up in multiple jurisdictions, may be used to obscure the audit trail of the funds (and thus, their origin and/or destination). Additionally, legal persons and arrangements also enable the concealment of the identity of the true beneficiary of the funds through multiple layers of ownership. In fact, criminals are known to use companies to move terrorist funds because these transfers attract less attention than the movement of funds between individuals.

Apart from private limited companies, which are vulnerable to exploitation, the features of trusts and foundations, like their significant privacy features and their international usage, also renders them attractive for FT purposes. Their shareholders are, more often than not, legal persons, making it even harder to track and reveal the beneficial owner(s) ('BOs'). Foundations are also afforded confidentiality by law, where their beneficiaries do not appear in public records.

Various techniques may be deployed to conceal beneficial ownership that may entail the involvement of numerous intermediaries. A common set-up is one consisting of several layers of companies and trusts across multiple jurisdictions, with ownership of each layer vested in different parent shell companies.

Another example of these complex structures includes companies set up in foreign jurisdictions with less regulation and which permit the usage of, e.g., bearer shares, and nominee shareholdings and trusts. These complex structures make it extremely difficult for persons to identify the true BO, albeit having a common controlling party and/or beneficiary.

2.6.2 Red Flags

Subject persons must take note of the following red flags to ensure that those customers that are legitimate businesses are not acting as a front for other persons with terrorist links:

- The use of needlessly complex structures consisting of legal persons, such as private companies, and other legal arrangements, such as trusts and/or foundations, attempting to disguise the BO(s).
- The involvement of multiple jurisdictions within one organisational set-up, particularly if accompanied by a complex structure, which appears to be unfounded.
- A series of complex transfers of funds involving various individuals as a means to hide the source and intended use of the funds.
- Transactions that are not economically justified and that fall outside the expected or usual activity of the legal person or arrangement.
- Fund transfers exclude the originator's information, or the person on whose behalf the transaction is conducted, when the inclusion of this information is usually expected.
- Fund transfers to persons or businesses in high-risk jurisdictions that appear to be unrelated or unfounded to the activities of the legal person or arrangement.
- The parties to a transaction are linked to areas of conflict, or to countries known to support terrorist organisations or activities, or those in close proximity thereto.
- The use and involvement of multiple bank accounts and/or multiple foreign bank accounts.
- The use of front and/or shell companies that are created purely to introduce an additional layer of concealment.

Case study 12

Suspicious activity involving a legal person

A restaurant manager, who held a banking account with a credit institution, regularly deposited significant amounts of cash into his bank account, and also received ample cheques drawn from a wooden pallet company (Company B). His account did not show the expected financial activity pertinent to his established profile, such as payment for food. This inconsistency led the credit institution to become suspicious and to submit an STR.

Furthermore, the credit institution noted that Company B's bank account showed significant cash withdrawals, ranging between €500,000 and €1 million, which gave further rise to their suspicion. The analysis revealed that the individuals concerned were linked to a terrorist organisation.

2.7 TRADE-BASED TERROR FINANCING

2.7.1 Vulnerabilities

An emerging trend that has been identified is one concerning terrorist financiers using fraudulent, trade-based practices to collect, transfer and utilise funds and assets for FT purposes. Owing to cash flow involved in trade as well as the international element of certain trade systems, this industry is subject to ample risks and vulnerabilities, which may give rise to trade-based FT, particularly because of the opportunity that trade gives to terrorists to transfer value and goods through seemingly legitimate trade channels.

Businesses and trades that are cash intensive may be used as vehicles of FT because it is easier to overstate income and funnel illicit money through these businesses, and to use front companies to conceal the movement of terrorist funds and disguise them as legitimate business transactions. Furthermore, criminals may also misuse the trade industry by generating sums of money through false invoices, particularly those relating to imports and exports.

Trades involving precious stones, such as the diamond trade, are particularly attractive to criminals and prone to exploitation owing to the opaque nature of the market, the high level of expertise required for this type of trade, its global nature and the high market value of these stones, which are also inherently attractive as a non-traceable, anonymous currency.

Similarly, valuable goods, such as precious metals (e.g. gold) or artwork, which are not typically subject to border declaration, are moved across borders with relative ease, and traded for currency or supplies. E.g., Hawala dealers are known to use gold to balance their books, as opposed to cash, since it does not raise the same amount of suspicion when being transported.

Case study 13

Fund transfers involving customers active in trade

In the space of a few months, a credit institution noted similar transactions concerning numerous and significant fund transfers to and from various jurisdictions in accounts held by three of its customers (Persons A and B, and Company C).

Soon after the opening of his account, Person B was noted to be the beneficiary of several bank cheques of large amounts in US dollars. Furthermore, Company C was also receiving large fund transfers in US dollars, originating from companies active in the diamond trade, which were debited into Company C's account via several transfers to the Middle East in favour of Person A, a European citizen born in Africa and residing in the Middle East. This led the credit institution to report the suspicious activity of these customers to the respective Financial Intelligence Unit ('FIU').

The credit institution also noted that one of Company C's directors, a European citizen residing in Africa, held an account at a European credit institution through which transfers took place to and from other countries in Europe, Africa, North America and the Middle East. The inward transfers made to this account were predominantly in US dollars, which were subsequently converted to Euro and used to make transfers to other countries and to accounts in the EU belonging to Person B and his wife. The company's largest transfers were mainly destined to the same person (Person A), also a Middle East resident.

It later transpired that both Person A and Person B were suspected of having purchased diamonds from the black market in Africa and smuggling them into the EU for the benefit of a terrorist organisation.

2.7.2 Red Flags

- The transactions of the customer who is involved in the trade industry appear to lack an economic rationale.
- The customer's financial activity is inconsistent with the usual practices in the trade. E.g., cheque deposits followed by similar amounts being withdrawn, foreign currency deposits followed by currency conversion and cash withdrawals in local currency,
- The product being purchased or sold as declared in an invoice does not match the activities of the purchasing business, or the customer's activities do not match his/her declarations. E.g., trade volumes are larger than the expected volumes.
- The customer's purchasing pattern does not make economic sense. E.g., several bank cards are used to make multiple purchases.
- The customer lacks a physical location or legitimate on-line presence. E.g., the address provided is a mail-box service or legal office or, in the case of a website, a landing page is provided with no real functionality and no manner to purchase listed products.
- The customer is a shell or front company, or is being suspected of being one for various reasons, such as being set up in a privacy haven jurisdiction.
- The customer is unwilling or reluctant to provide the requested trade documentation.
- The customer conducts or receives fund transfers to or from countries that are higher risk for Black Market Peso Exchange activity, including but not limited to Mexico, Guatemala, Uruguay, Argentina, Paraguay, Brazil and Venezuela.
- The customer does not provide any information to explain transfers that appear to be unfounded.
- Transactions made by the customer, at any stage of the trade, involve persons related to high-risk jurisdictions, which are unrelated to the particular trade. E.g., a person trading in certain industries is expected to be involved with certain higher risk jurisdictions.
- Customers, particularly businesses, which pay a sales order up front when the customary payment date is within an extended term since this is not usual business practice.
- The trade dealer does not appear to be familiar with trade practices and maintains a high level of secrecy.
- The customer is sending funds to an unusually large variety and number of recipients, especially if this is done following the receipt or deposit of funds.

Case study 14

Importation of second-hand vehicles

A scheme was discovered involving money being funnelled through the sale of second-hand vehicles. Funds were being transferred from a high-risk jurisdiction to a reputable jurisdiction to purchase and transport the cars to other high-risk jurisdictions for re-sale.

Following the re-sale, the cash proceeds generated were being transferred through bulk cash smuggling to the high-risk jurisdiction from which the funds to purchase the vehicles originated. These funds were smuggled along with other proceeds derived from illegalities, such as narcotics trafficking.

While this case may appear to be one related to ML, on further analysis, the involvement of a particular, renowned terrorist group was identified in various stages of the scheme, particularly to sell narcotics and smuggle the proceeds generated from their sale, as well as the sales of the used cars.

Subject persons dealing with customers who engage in trade transactions, especially higher risk ones, must ensure that they understand the respective trade finance activities to be able to detect suspicious or unusual activities that may be linked to FT. It is recommended that these subject persons engage a financial crimes expert who has knowledge of trade-based money laundering and how it can be used for FT so that they can be in a better position to identify customers who are effecting these suspicious or unusual transactions.

3. EMERGING FT TRENDS IN MALTA

The following emerging trends have been identified as being indicative of FT that may be connected to or are taking place in Malta. In isolation, the activities listed below would usually be harmless, unless they coincide with activities typically associated with terrorists, such as travel or purchase of travel arrangements to or from jurisdictions where terrorist groups are known to operate or other conflict zones, or if the withdrawals are carried out from these jurisdictions. These indicators may assist subject persons to better identify suspicious activity and report it immediately:

- Inflated salaries, which seem excessive in comparison with the market rate for remuneration for similar roles. This could be an indicator of the movement of illicit funds.
- Encashment by customers of "only" cheques issued in the name of third parties, especially cheques relating to salary payments or social security benefits.
- The cashing out of a number of cheques by customers issued in the name of third parties, since this may be indicative of carrying out unlicensed banking activity.
- Remitting money to locations that are in, or adjacent to, conflict zones or areas where terrorism activity is known to be present, without apparent family or business connections to those places.
- Remitting money to persons or entities (including non-governmental organisations) with suspected links to terrorism.
- A large volume of cash deposits that are not in line with the customer's known profile.
- The customer becomes uncooperative when requested to provide the required details and/or documentation on a transaction or operation, or provides documentation that may not be authentic or raises suspicion.
- A number of airline tickets are purchased by the customer, whether for themselves or for others, and whether the flights are direct or connecting, to jurisdictions that are identified as conflict zones or in proximity to these jurisdictions, especially without having any apparent familial or business connections in those places.
- The customer's transaction activity is unexplained or inconsistent with the customer's known profile.
- The customer's transactions may be indicative of terrorist related activities, such as recurring purchases from camping or survival stores, first-person shooting games or combat training-type activities, and especially if these coincide with the customer's travel arrangements to conflict zones or those adjacent thereto.
- The customer sells a significant part of, or all, their personal assets followed by travel and/or transactional activity to conflict zones or areas where terrorism activity is known to be active.
- The customer acquires loans, towards which no or insignificant payments are made, followed by travel and/or transactional activity to conflict zones or areas where terrorism activity is known to be active.
- The customer withdraws or receives funds from locations that are in, or adjacent to, conflict zones or areas where terrorism activity is known to be present, without apparent family or business connections to those places.
- The customer requests payment of proceeds of or receives funds from unrelated third parties and does not provide supporting documentation for this and/or becomes hesitant when questioned about them. These unrelated third parties may be accomplices or vulnerable persons who have been taken advantage of.
- The customer's transaction narrative is suspicious and/or does not make any commercial sense within the context of the transaction itself.

CONCLUDING REMARKS

Subject persons are hereby reminded that:

(i) The indicators listed above are not exhaustive and a customer may exhibit other indicators that will link them to FT.

(ii) This Guidance Document should be read in conjunction with Section 3.2 and Section 3.5 of the Implementing Procedures Part I on Risk Factors.

(iii) Subject persons must be on the alert and refuse to provide services to or facilitate the transfers of assets involving individuals and/or entities that are subject to international or EU sanctions. Therefore, subject persons must exercise caution in relation to those persons identified as related to terror by reputable designated lists of terror groups issued outside the EU, e.g., under the United Nations Security Council Resolution 1373, such as the sanctions list issued by the US Office of Foreign Assets Control). It is crucial that subject persons screen their client base regularly against lists of sanctioned individuals and entities, as well as whenever updated or new lists are issued. Subject persons should thus ensure that they keep updated with any sanctions that may be imposed and with any guidance, notices, decisions, recommendations or rulings that may be issued by the SMB. Reference should be made to Section 4.11 of the Implementing Procedures Part I on Sanctions Screening for further guidance.

(iv) Subject persons are reminded to carry out open searches on their customers or potential customers. This includes conducting searches on any personal identifiable information relating to the same and, where applicable, on the usage of any usernames that come to the attention of the subject person.

(v) In their transaction monitoring, subject persons are to evaluate whether the customer's transactions (including a company's business activities) make economic and/or logical sense. Vigilance should be exercised when the customer's transactions result in or demonstrate significant losses.

(vi) Vigilance should also be exercised when the customer or persons linked to the customer have been the subject of adverse media or law enforcement information that links them to terrorist groups or terrorist activities.

(vii) Subject persons should likewise be wary of customers transacting with individuals or entities that have been identified by reputable media sources or sanctions lists as being linked to terrorist organisations or terrorist activities.

(viii) Developing an understanding of the expected transactional activity and patterns of persons of different nationalities would assist subject persons to determine behaviour that falls within and outside the norm.

(ix) Vigilance should be exercised when the customer's IP logins indicate areas of conflict or those in close proximity thereto.

(x) Vigilance should be exercised in the case of customers who have links with or have been identified by media or law enforcement as having travelled, attempted or intended to travel to high-risk jurisdictions, such as:

a) those locations which are in the midst of, or adjacent to, armed conflict, where terrorists are known to operate;
b) those locations that are known to support terrorist activities or organisations;
c) those locations that are known to be politically unstable; and
d) those jurisdictions that have been identified as having weaker ML/FT controls.

(xi) Vigilance should be exercised in the case of persons who purchase real estate in locations in proximity to or in the midst of armed conflict where terrorist groups are known to operate or other jurisdictions that are subject to weaker ML/FT controls, those who liquidate a significant amount of their personal assets without any justification (e.g., selling one's residential home, liquidating any retirement plans or withdrawing all funds held in one's bank accounts), and where there is information about the customer that indicates a possible connection with terror organisations.

(xii) Atypical activity by a customer may be a sign of ML and/or FT. However, given that in the case of FT – especially in the case of lone actors – a transaction's value may be significantly lower than usual, the application of thresholds for ongoing monitoring purposes may limit a subject person's ability to detect them. Thus, when carrying out ongoing monitoring, subject persons are also to consider low-value transactions that may or may not be accompanied by one or more of the red flags listed above.

(xiii) Subject persons that provide payment services are reminded to adhere to the Funds Transfer Regulation and the FIAU's Guidance Document on Transfers of Funds having Missing or Incomplete Information.

(xiv) Any risk assessment carried out by subject persons, as well as any measures, policies, controls and procedures adopted by them in terms of Regulation 5(5) of the PMLFTR, are to also consider FT risks. Reference should be made to Section 3.2.7 of the Implementing Procedures Part I on the sources of information that are to be consulted to determine risk factors. Direct or indirect links with areas known for terrorist activity and/or support and/or activities known to be used by terrorist groups to finance themselves should receive due consideration whenever a risk assessment is carried out.

(xv) Subject persons are to keep abreast of developments to be aware of which jurisdictions are exposed to terrorism or are suspected of supporting terrorists and terrorist organisations. A jurisdiction can be considered as supporting terrorists and terrorist organisations independently of whether any such support is provided by state authorities or private individuals.

(xvi) Cases indicative of ML may also be indicative of FT.

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

This includes a thorough reading and understanding of any results that may be published following national risk assessments. Moreover, they are encouraged to attend training and read material published by esteemed international or regional bodies that will assist them in enhancing their knowledge on the subject in question. This includes, e.g., publications made available by the FATF and Europol. Only by doing so can subject persons develop their own, business-specific red flags based on their institutional risk assessments and thus be in a position to prevent their business from being used for FT purposes.

65C, Tower Street,
Birkirkara BKR 4012,
Malta

Questions on this document or on the application of AML/CFT measures may be sent to **queries@fiaumalta.org**

Financial Intelligence Analysis Unit
65C, Tower Street,
Birkirkara BKR 4012,
Malta

Telephone: (+356) 21 231 333
Fax: (+356) 21 231 090
E-mail: info@fiaumalta.org
Website: www.fiaumalta.org