Gibraltar Financial Intelligence Unit
HM Government of Gibraltar

Counter Terrorist Financing

Guidance Notes

February 2021 – Version 1.0

Table of Contents

Introduction and Scope

Terrorism remains a significant threat to international peace, security and economic stability across all regions of the globe. Combating the financing of terrorism has for many years been a central element of the international community's response to this threat.

Terrorist financing (TF) activity is extremely hard to detect, not just because it may involve smaller sums of money than money laundering activity, but because it involves transactions that are often indistinguishable from legitimate day-to-day activities. Terrorist groups such as Al-Qaeda and their affiliates obtain funding from a wide and continually evolving range of sources. This funding is used to conduct terrorist acts and maintain and grow their terrorist organisations as a whole.

The Financial Action Task Force (FATF) of the United Nations Security Council has been at the forefront of setting international standards to counter terrorist financing (CTF), the purpose of which is to deprive terrorists of funds and their resources. Gibraltar's legislative framework is designed to align with these standards.

Extreme right-wing terrorism (also referred to as 'far right, or ethnically and racially motivated terrorism') is not a new phenomenon but there has been a recent revival of right-wing extremist groups and an increase in frequency of attacks, with deadly results. This guidance includes a section on right-wing terrorism but further research will be needed to provide a more detailed analysis on relevant red flags and indicators.

Whilst the overall threat of TF in Gibraltar at a jurisdictional level remains low, the risk is higher for specific sectors of the economy or when dealing with certain jurisdictions. An effective CTF response requires that all stakeholders have a robust understanding of their obligations together with the TF risks faced in Gibraltar and, more specifically, the threats faced in their industry.

This guidance has been prepared by the Gibraltar Financial Intelligence Unit (GFIU). It aims to provide entities with guidance on their CTF obligations and sector specific guidance on the TF threats they face.

Chapter 1 provides a high level and non-jurisdiction-specific introduction to TF[1];

Chapter 2 outlines the CTF obligations that are applicable in Gibraltar;

Chapter 3 sets out the jurisdictional risks of TF in Gibraltar;

Chapter 4 provides sector-specific guidance on the TF threats faced, including case studies and known risk indicators;

Chapter 5 describes the ways in which GFIU will provide local contextual information and provide feedback to reporting entities on their suspicious activity reports.

This guidance takes into account the 2020 National Risk Assessment for AML/CFT and PF conducted by the national coordinator for AML/CFT. It also draws on various FATF publications with their permission, which is gratefully acknowledged. The reader's attention is drawn to these where appropriate for their further information.

[1] Chapter 1 closely reflects the information set out in the 2015 FATF report, "Emerging Terrorist Financing Risks".

Please note that neither GFIU nor the Gibraltar competent authorities can issue definitive guidance on how the law might be applied in a particular case or how the courts might interpret the law. Please also note that the relevant competent authorities in Gibraltar would consider each matter on the facts and the specific legal requirements that apply.

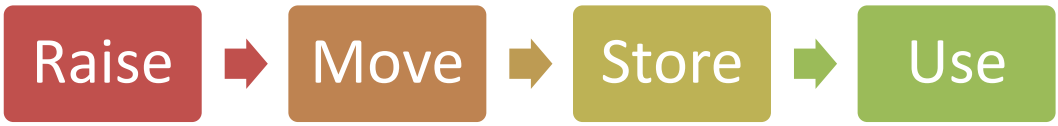
This guidance is not intended to be, and should not be relied on as legal advice. GFIU strongly advises you to refer to the relevant, up-to-date legislation. If you are unsure about your obligations, you are strongly encouraged to obtain independent legal advice. This guidance may be updated from time to time. Always check that you are referring to the latest version.

Brexit

Gibraltar, together with the UK, left the European Union on the 31st January 2019 ('Brexit'). The transition period agreed as part of the UK-EU Withdrawal Agreement, which applied to Gibraltar, ended on the 31st December 2020. Prior to this, Gibraltar's legislative framework implemented EU law where it existed and gave direct effect to EU sanctions in Gibraltar. This remains the case and Gibraltar law continues to reflect the EU framework notwithstanding the expiry of the transition period. In addition, the Sanctions Act 2019 recognizes, as a matter of Gibraltar domestic law, new EU sanctions promulgated since 1st January 2021.

1 Overview of terrorist financing

The key stages of TF are the raising of funds, the movement of funds, the storing of funds and the use of funds. Subsections 1.1 – 1.3 deal with raising, movement and use of funds as they apply to terrorist organisations (TOs). TOs are usually large, structured groups that may or may not control territory in certain countries. Special considerations apply to small cells and lone actors, as well as foreign terrorist fighters (FTFs). These topics are addressed in subsections 1.4 and 1.5 respectively.



1.1 How do terrorist organisations spend their funds?

TOs invariably require funding to prepare and carry out their plots and to support the full range of activities that they engage in. The overall financial requirements to maintain their infrastructure, personnel and activities are usually very high, especially in large TOs. Their ability to operate and further their objectives is therefore directly linked to their ability to secure reliable funding.

Areas of expenditure for terrorist organisations	
Operations	Funding is required to prepare for and execute specific attacks and other activities that further their ideological aims. This often includes travel to and from the target location, living expenses such as accommodation, food and medical treatment, the use of vehicles and other equipment and the purchase of arms, including improvised explosive devices (IEDs).
Propaganda & Recruitment	Funding is required to recruit members and support other fundraising activities. The internet has proved to be an invaluable and cost effective tool for TOs to increase their reach and solicit funds from their supporters. Social media is a particularly attractive channel and its exploitation for the purposes of recruitment, propaganda and fundraising has become a priority CTF issue. Larger and more sophisticated TOs are investing in sophisticated propaganda operations that include publishing magazines, newspapers and websites and even acquiring television and radio outlets.
Training	Funding is required to train personnel and sympathisers in a range of areas, including weapons training, bomb-making, clandestine communication and ideology. Training can take place remotely, over the internet or in face-to-face camps, where the TO will often acquire land and buildings to provide a safe haven for such purposes.

Salaries & Member Compensation	Funding is required to provide financial security and incentives to the TO's leadership and its members and to provide financial support to the families of deceased or jailed operatives. Doing so helps to ensure members' commitment to the TO's objectives and ideology.
Social Services	Funding is often used to establish or subsidise local health, social or educational services. This serves to undermine the credibility of legitimate governments, build support within local populations and aid recruitment efforts.

TOs must have the skills necessary to obtain, move, store and ultimately use the financial resources required to meet their aims. Financial management in TOs requires planning and accounting for all resources and assets that the group controls. Large TOs will often rely on terrorist financial managers to accumulate revenue, establish financial shelters and oversea financial disbursements. Groups such as ISIL have actively recruited accountants and other financial professionals to monitor the activities of financial entities within their control. Smaller TOs and cells also require financial management, but this may take place in a less formal manner and without having a fully dedicated and qualified member exclusively assigned to that function.

1.2 How do terrorist organisations raise funds?

TOs often rely on numerous sources of income. Some sources will be inherently illegitimate, such as criminal activity. Others may come from ordinarily legitimate activities which nevertheless become illegitimate by virtue of their underlying terrorist purpose. This places unique challenges on CTF efforts and distinguishes TF from money laundering (ML), in which the aim is always to launder the proceeds of crime.

Known fundraising methods include:

- **Private donations** - Private donations can come from a variety of sources, including direct financial support from individuals. TOs can use social media networks and crowdfunding platforms as vehicles to solicit, receive and move donations from sympathisers across the globe. An online fundraising scheme may involve up to several thousand sponsors and raise large amounts of cash.

Case Study: Social network fundraising with prepaid card

Individuals associated with ISIL called for donations via Twitter and asked the donors to contact them through Skype. Once on Skype, those individuals asked donors to buy an international prepaid card (a credit for mobile phone or the purchase of an Apple or other programs or credit for playing on the Internet) and send them the number of this prepaid card via Skype. Then, the fundraiser sent this card number to one of his followers in a neighbouring country from Syria, who would sell this card number at a lower price and give the cash proceeds to ISIL.

Source: FATF Emerging Terrorist Financing Risks 2015

- **Abuse of non-profit organisations (NPOs)** - Abuse of NPOs is a significant problem and can involve:

    - diverting legitimate donations through affiliated individuals to TOs;
    - creating false or sham NPOs to obtain funding from unwitting donors;
    - abusing a NPO's program implementation to aid the TO;
    - using it to support recruitment into TOs and
    - exploiting NPO authorities.

  NPOs most at threat are those engaged in service activities which operate in close proximity to an active terrorist threat and 'correspondent' NPOs, which send funds that have been raised in other regions to them.

- **Funds brought by foreign terrorist fighters (FTFs)** - FTFs that have been recruited abroad may bring cash or other funds in order to support the TO's cause. These funds may have been obtained through otherwise legitimate activity, such as employment or personal savings. Alternatively, the FTF may have applied for a small loan or state benefit with no intention of using the money for its legitimate purpose and with no intention of paying it back.

- **Trade in natural resources such as oil, metals and minerals** - Land controlling TO's will often seek to exploit the natural resources within their territory to further their objectives. This can involve extracting and/or refining the resources themselves or levying taxes on companies that directly engage in this activity. Alternatively, they may tax trade and smuggling routes within their area of control.

- **Legitimate business** - Legitimate businesses can be established or acquired by TOs via proxies and then used as a source of funding. Used car dealerships and restaurant franchises have been found to be used for this purpose, however the risk applies across all sectors. There is a particular risk in sectors which do not require formal qualifications and where starting a business does not require substantial investments. The risk that a business will divert funds to support terrorist activity is greater where the relation between sales reported and actual sales is difficult to verify, as is the case with cash-intensive businesses.

- **Self-funding** - Smaller cells with more limited ambitions and which are settled within their target country or neighbouring ones may be able to fund their operations themselves. This could be from legitimate means, by involvement in criminal activity or the abuse of loan facilities or state benefits. Their needs to move value across large distances or in large quantities will be far lower than that of a large TO, making their financing activity particularly difficult to detect and disrupt. See section 1.4 below.

- **State support** - A TO may benefit from external state sponsorship. Whilst accusations of state sponsorship are normally highly controversial, there have been instances where countries have not hesitated to designate others as state sponsors of terrorism.

- **Involvement in criminal activities** - TOs may engage in a wide range of criminal activities to raise funds or they may collaborate with organised crime groups

(OCGs) for this purpose. Such criminal activities can include extortion, robberies, looting, cattle/livestock rustling, kidnapping for ransom, trafficking of drugs, weapons and other goods (such as antiques), trafficking of migrants and persons, oil and cigarette smuggling, piracy, cybercrime and fraud.

1.3 How to terrorist organisations move funds?

The movement of terrorist funds from the place where they are raised or held to where they will be ultimately used represents both a critical step in the TF process and an important opportunity to detect and disrupt TF through robust CFT measures.

Known methods of moving terrorist funds include:

- **Funds transfers through banks** - The banking sector is an attractive means for TOs to move funds globally due to the speed and ease with which they can move them and the sheer size and scope of the financial system, which gives them the opportunity to blend in with normal financial activity. One way TOs do this is through trade-based money laundering, in which legitimate, false or manipulated trade transactions are used to disguise movements of terrorist funds. While AML/CFT measures are making it more difficult for the financial sector to be used for TF purposes, the risk remains prevalent.

- **Money value transfer systems (MVTS)** - MVTS refers to financial services that involve the acceptance of cash, cheques, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network to which the MVTS provider belongs. Transactions performed by such services can involve one or more intermediaries and a final payment to a third party, and may include any new payment methods. Migrant communities and families rely heavily on MVTS to remit funds home, which provide TOs with a channel for commingling TF with legitimate family transfers that is difficult to detect. Remittance providers are especially vulnerable where they are unregulated and not subject to AML/CFT supervision. The biggest threat involves corrupted and complicit agents or employees who knowingly facilitate and obfuscate TF transfers on behalf of TOs.

Case Study: Complicit MVTS Agent

An individual raised funds for Al-Shabaab from within the Somali diaspora in Missouri and elsewhere and used a variety of licensed money service businesses (MSBs) with offices in the United States to remit the money to Somalia for general support of Al-Shabaab fighters. The co-conspirator, who worked for one of the MSBs involved, helped the individual avoid leaving a paper trail by structuring transactions into low dollar amounts and by using false identification information. The MSB worker and other conspirators used fictitious names and phone numbers to hide the nature of their transactions.

Source: FATF Emerging Terrorist Financing Risks 2015

- **Physical transportation of cash** - Funds are often converted into cash to be smuggled to conflict zones, which continues to be a prevalent and hard to detect method for the movement of terrorist funds, especially in countries in or next to high risk areas and those that have informal and unregulated economies or porous national borders. Cash is still the predominant method used by TOs to fund their organisations and operations.

- **Virtual currencies** – A Virtual Currency (VC) is a digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value. At present they do not have legal tender status in any jurisdiction and are instead considered as a virtual asset (VA). Whilst virtual currencies such as bitcoin allow for the anonymous transfer of funds internationally, the opportunities for spending them are severely limited as compared with cash. This is believed to help account for the fact that a 2018 report by the European Parliament found that the adoption of virtual currencies by TOs did not appear to be widespread. However, should their adoption become more widespread, this may lead to greater use by TOs. At present, virtual currencies' main risks are their use as a currency for to receive online donations for terrorist causes and the purchase of illicit items such as weapons or fraudulent documents using the dark web.

- **Prepaid cards** - Prepaid cards are cards that are preloaded with a fixed amount of electronic currency or value. The category of most concern is open loop prepaid cards, whereby the holder is able to withdraw funds from ATMs worldwide and engage in transactions with any merchant or service provider participating in the payment network. Prepaid cards are replacing travellers' cheques as a method of moving money offshore. They can be loaded domestically via cash or other non-reportable methods and carried or posted abroad more easily and securely than cash. The funds can then be converted back to cash through multiple offshore ATM withdrawals.

- **Internet based payment services** - Internet-based payment services provide mechanisms for customers to access, via the Internet, pre-funded accounts which can be used to transfer the electronic money or value held in those accounts to other individuals or businesses which also hold accounts with the same provider. Cases involving low-value transactions via online payment systems such as PayPal have been linked to a number of terrorism suspects, however the extent to which these accounts have been used to finance terrorism is unclear.

- **Smuggling of goods** - TOs are able to move value undetected by smuggling goods across international borders. Natural resources and high value items, such as antiques are known to be used by TOs for this purpose.

- **Trade-based money laundering -** trade-based money laundering is defined as the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimise their illicit origins. In practice, this can be achieved through the misrepresentation of the price, quantity or quality of imports or exports. Moreover, trade-based money laundering techniques vary in complexity and are frequently used in

combination with other money laundering techniques to further obscure the money trail.

1.4 Small cells and lone actors

Small cells and lone actors pose a significant terrorist risk, yet they also present distinct challenges with regards to CTF efforts. Their financial requirements are often low and in many cases they are able to self-fund their operations through legitimate activities such as employment income or personal savings. Their activities often require fewer and smaller financial transfers and movements of funds. Furthermore, these groups may be domiciled in and/or comprised of nationals of their target countries, and their activities often require fewer and smaller financial transfers and movements of funds (if any at all). These factors make it extremely difficult, if not impossible, to detect their financing activities and pre-emptively disrupt their operations through CTF measures and efforts.

1.4.1 The rise of right-wing terrorism

Whilst the main focus in analysing the threat of small cells and lone actors has traditionally been on Jihadist terrorism, which accounts for the largest number of attacks, the threat posed is by no means confined to a particular religion or ideology, and it is important to note in particular the proliferation of right wing terrorism in recent years. A large number of extreme right wing attacks in Europe have been committed by groups or individuals that may not necessarily be connected to known extreme right wing groups or networks. As a result, the threat from small cells or lone actors becomes more prevalent. In their first public briefing since far-right terrorists murdered the Labour MP Jo Cox in 2016 and murdered a Muslim worshipper near a north London mosque in 2017, the British police revealed:

1. A quarter of all terrorism arrests between September 2018 to September 2019 were linked to far-right violence;
2. The far-right caseload of counter-terrorism police jumped from 6% to 10% from the start of 2018 until September 2019;
3. Referrals to Prevent, an anti-radicalisation programme in the UK, had almost doubled between 2016 and 2018 for the far right, from 10% to 18%, and were expected to rise further;
4. A third of all terror plots to kill in Britain for the period January 2017 until September 2019 – seven out of 22 – were by those driven by extreme-right causes.

Whilst the majority of right-wing attacks have been committed by lone actors and small cells, the financing of which plays a far smaller role for the reasons given above, the plots often nonetheless have a financial dimension – the purchase of a knife or the hire of a van, for example. Furthermore, finance plays an important role in enhancing the promotional activity of extreme right-wing groups, from creating propaganda to organising marches and events to maintaining websites supporting and promoting extremist literature and exchanges of ideas. Such groups may not themselves engage in or advocate terrorist activity, but it has been suggested that non-violent extremism is often the first step in a process of radicalisation that ends in terrorism. These groups

tend to raise money from private donations, fundraising events and the sale of merchandise.[2] Other red flags can also include individuals purchasing items related to extreme right wing merchandise, such as symbols and literature.

1.5 Foreign Terrorist Fighters

FTF's are individuals who travel to conflict zones in order to join and actively support a terrorist organisation or cause. While they are not considered to be a significant source of funding, they contribute to the larger TF threat posed by these groups. More importantly, FTFs are considered one of the main forms of material support to terrorist groups, and thus remain a significant TF threat.

The funding needs of FTFs are generally modest and include transportation, accommodation while in route, outdoor clothing, camping goods, mobile phone/plans, food and other general living expenses. FTFs are likely to have some expenditure requirements just prior to entering the conflict zone, including the purchase of weapons. In some early instances, FTFs were relied on to bring additional funds with them when they joined the terrorist group. However, in the current context, FTFs appear to be more valuable as human resources than as funds-providers.

Self-funding by individuals and funding by recruitment/facilitation networks are considered the two most common methods used to raise funds for FTFs. With regards to self- funding, individuals often use funds from legitimate sources (e.g. employment income, social assistance, family support, bank loans) to finance their travel to the conflict zone. In some cases, investigations have revealed that small businesses were intentionally established and used to generate revenue that supported FTF travel. Some jurisdictions have also noted the sudden sale of assets including personal belongings and assets purchased on credit just prior to the FTFs planned travel. In this respect, there are some similarities between FTFs and small terrorist cells. Family and associates have also knowingly or unwittingly transferred their own legitimately obtained funds to persons engaged in conflict.

Recruitment networks and individuals facilitate FTFs to travel to conflict zones and join terrorist groups. Family, friends or facilitation networks also provide financial support to FTFs once they depart for the conflict zone. It appears that most groups are informal or ad hoc, depending on what assistance is required by the FTF and there are often links between facilitators in the home country and areas bordering the conflict zone.

[2] For more information, see Tom Keatinge, Florence Keen & Kayla Izenman (2019) Fundraising for Right-Wing Extremist Movements, The RUSI Journal, 164:2, 10-23, DOI: 10.1080/03071847.2019.1621479

2 Counter Terrorist Financing Obligations

2.1 Domestic Obligations

The CFT obligations under Gibraltar law are contained in the Proceeds of Crime Act 2015 (POCA), the Terrorism Act 2018, the Counter-Terrorism Act 2010, the Terrorist Asset-Freezing Regulations 2011 and the Sanctions Act 2019.

2.1.1 Due diligence, record-keeping, procedures and training

Part III of POCA sets out key obligations with regards to customer due diligence (CDD), record-keeping, the establishment of procedures to combat AML/TF and the relevant training of staff. These obligations apply to relevant financial businesses, which are businesses that engage in one or more of the following business activities:

1. electronic money issuer or deposit-taking business carried on by a person who is for the time being an authorised institution under the Financial Services Act;
2. business of the Savings Bank or of the Gibraltar International Bank;
3. any home regulated activity carried on by a European institution;
4. investment business within the meaning of the Financial Services Act;
5. any of the activities in points 1 to 12 or 14 of the Annex I to the Consolidated Banking Directive other than an activity falling within paragraphs (a) to (e);
6. insurance business carried on by a person who has received official authorisation pursuant to Article 6 or 27 of the First Life Directive;
7. auditors, insolvency practitioners, external accountants and tax advisors;
8. estate agents and letting agents;
9. art market participants;
10. notaries and other independent legal professionals, when they participate whether–
    a. by assisting in the planning or execution of transactions for their client concerning the–
        i. buying and selling of real property or business entities;
        ii. managing of client money, securities or other assets;
        iii. opening or management of bank, savings or securities accounts;
        iv. organisations of contributions necessary for the creation, operation or management of companies;
        v. creation, operation or management of trusts, companies, foundations, or similar structures; or
    b. by acting on behalf of and for their client in any financial or real estate transaction;
11. controlled activity other than a general insurance intermediator under the Financial Services Act;
12. dealers in all high value goods whenever payment is made or received in cash and in an amount of 10,000 euro or more;
13. gambling services;
14. currency exchange offices / bureaux de change;
15. money transmission / remittance offices,
16. any recognised or authorised scheme or any authorised restricted activity under the Financial Services Act.

17. any other financial institution; or
18. undertakings that receive, whether on their own account or on behalf of another person, proceeds in any form from the sale of tokenised digital assets involving the use of distributed ledger technology or a similar means of recording a digital representation of an asset.

The key to effective CTF is to have sound measures and procedures in place to comply with CDD measures, since this will enable relevant persons to "know their clients" and understand the possible significance of transactions in the context of CTF.

The requirements under Part III are extensive and it is beyond the scope of this note to provide detailed guidance on their application to each sector of Gibraltar's economy. Instead, operators are advised to refer to any guidance published by their supervisory authority on this topic.

The Financial Services Commission (FSC) has published guidance that is to be treated as having been issued by the following supervisory authorities:

- the Financial Services Commission;
- the Authority appointed under Section 2(1) of the Financial Services (Investment and Fiduciary Services) Act;
- the Commissioner of Banking and the Banking Supervisor;
- the Commissioner of Insurance and the Insurance Supervisor.
- the Financial Secretary, or such other person or entity as may from time to time be designated by the Minister for Finance by notice in the Gazette in respect of relevant financial businesses to which section 9(1) applies and which are not supervised by a body listed above.

The guidance, which applies to any organisation regulated by any of the above entities, can be found here.

The Gambling Commissioner has published a code of practice for the remote gambling industry. It can be found here.

The Office of Fair Trading has published guidance notes for High Value Dealers. They can be found here.

It has also published guidance notes for Real Estate Agents, which can be found here.

The Registrar of the Supreme Court has published guidance for the legal sector. It can be found here.

Applying the risk-based approach to terrorist financing

A key theme of the POCA regime is the need for relevant financial businesses to apply a risk-based approach (RBA) to anti money laundering (AML) and TF. The RBA must be underpinned by an appropriately conducted risk assessment. This topic is addressed in each of the above guidance documents, however, FATF has produced specific guidance to assist all operators with regards to the TF element of their risk assessments. This can be found here.

All relevant financial businesses should read have and have regard to that guidance note when conducting their risk assessments.

FATF has also produced several guidance notes aimed at assisting various sectors in applying a risk based approach. Whilst their main focus is on AML, they also contain important information with regards to TF:

Sector	Link
Banking sector	https://www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Banking-Sector.pdf
Virtual currencies	https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf
Virtual asset service providers	http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf
Legal Professionals	https://www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Legal-Professionals.pdf
Accounting Profession	https://www.fatf-gafi.org/media/fatf/documents/reports/RBA-Accounting-Profession.pdf
Real Estate Agents	https://www.fatf-gafi.org/media/fatf/documents/reports/RBA%20Guidance%20for%20Real%20Estate%20Agents.pdf
Trust and Company Service Providers	https://www.fatf-gafi.org/media/fatf/documents/reports/RBA-Trust-Company-Service-Providers.pdf
Money or Money Value Transfer Services	http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-money-value-transfer-services.pdf
Prepaid Cards, Mobile Payments and Internet-Based Payment Services	http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf
Casinos (Land Based)	http://www.fatf-gafi.org/media/fatf/documents/reports/RBA%20for%20Casinos.pdf http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf
Life Insurance Sector	http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/RBA-Life-Insurance.pdf

Securities Sector	http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/RBA-Securities-Sector.pdf

2.1.2 Criminal Offences

Part 4 of the Terrorism Act defines various TF offences. They apply to all persons. This also includes all companies irrespective of whether or not they are regulated.

TF Offence	Particulars
Section 35 - Raising funds for terrorism	A person commits an offence if they receive money or other property or invite another to provide money or other property and they intend that it should be used, or have reasonable cause to suspect that it may be used, in full or in part, for the purposes of terrorism. A person also commits an offence if they provide money or other property and know or have reasonable cause to suspect that it will or may be used, in full or in part, for the purposes of terrorism. Providing money includes giving it, lending it or otherwise making it available whether or not in return for anything else.
Section 36 - Use and possession of money or other property for terrorism	A person commits an offence if they use money or other property for the purposes of terrorism or they possess money or other property and intend that it should be used, or have reasonable cause to suspect that it may be used, for the purposes of terrorism.
Section 37 - Arranging funds for terrorism	A person commits an offence if they enter into or become concerned in an arrangement as a result of which money or other property is made available or is to be made available to another and they know or have reasonable cause to suspect that it will or may be used for the purposes of terrorism.
Section 38 - Insurance against payments made in response to terrorist demands	An insurer under an insurance contract commits an offence if they make a payment under the contract, or purportedly under it, and the payment is made in respect of any money or other property that has been, or is to be, handed over in response to a demand made wholly or partly for the purposes of terrorism and they or the person authorising the payment on their behalf knows or has reasonable cause to suspect that the money or other property has been, or is to be, handed over in response to such a demand.
Section 39 - Money laundering	A person commits an offence if they enter into or become concerned in an arrangement of terrorist property by concealment, by removal from the jurisdiction, by transfer to nominees or in another other way which facilitates the retention or control by or on behalf of another person of such property.

	It is defence for a person charged under this section to prove that they did not know and had no reasonable cause to suspect that the arrangement related to terrorist property.
Sections 40 and 46 – Reporting Obligations	Sections 40 and 46 create offences that are committed if certain persons fail to disclose knowledge about the commission of a TF offence. Please see section 2.1.3 below for more information.
Section 49 – Tipping off offence	Section 49 creates a tipping off offence. Please see section 2.1.3 below for more information.

Part 4 also sets out some important defences to the TF Offences:

Defence	Particulars
Section 42 - Cooperation with police	A person does not commit a TF offence if he is acting with the express consent of a police officer. A person does not commit a TF offence by involvement in a transaction or arrangement relating to money or other property if he discloses to a police officer his suspicion or belief that the money or other property is terrorist property and the information on which his suspicion or belief is based. This defence only applies if the disclosure is made by the person after becoming concerned in the transaction, on their own initiative and as soon as reasonably practicable. This defence does not apply if a police officer forbids the person in question to continue their involvement in the transaction or arrangement and they fail to follow that instruction. Where a person is in employment his employer has established a procedure for the making of disclosures then the requirements for this defence can be complied with by making a disclosure to their employer rather than a police officer.
Section 43 - Arrangements with prior consent	A person does not commit a TF offence by involvement in a transaction or an arrangement relating to money or other property if, before becoming involved, the person discloses to an authorised officer the person's suspicion or belief that the money or other property is terrorist property together with the information on which the suspicion or belief is based and has the authorised officer's consent to becoming involved in the transaction or arrangement. A person is treated as having an authorised officer's consent if before the end of the notice period the person does not receive notice from an authorised officer that consent is refused. The notice period is the period of 14 working days starting with the first working day after the person makes the disclosure. An authorised officer includes: 1. A police officer, including those within GFIU; 2. A customs officer, including those within GFIU; 3. The head of GFIU; 4. Any other person authorised by the Head of GFIU for the purposes of this defence

	It is a defence for any person charged with a TF offence to prove that they intended to make a disclosure under this section and there is a reasonable excuse for their failure to do so.
Section 44 - Disclosure after entering into arrangements	A person does not commit a TF offence by involvement in a transaction or an arrangement relating to money or other property if, after becoming involved, the person discloses to an authorised officer their suspicion or belief that the money or other property is terrorist property together with the information on which the suspicion or belief is based. An authorised officer includes: 1. A police officer, including those within GFIU; 2. A customs officer, including those within GFIU; This defence is only available where there is a reasonable excuse for the person's failure to make the disclosure before becoming involved in the transaction or arrangement and the disclosure is made on the person's own initiative and as soon as it is reasonably practicable for them to do so. This defence does not apply if an authorised officer forbids the person in question to continue their involvement in the transaction or arrangement and they fail to follow that instruction. It is a defence for any person charged with a TF offence to prove that they intended to make a disclosure under this section and there is a reasonable excuse for their failure to do so.

A person must obtain the necessary consents in order to be entitled to the defences set out in sections 42 or 43 of Terrorism Act. The term 'consent' is frequently misinterpreted. Often it is seen as seeking 'permission' to proceed or confirmation that the funds are clean or that there is no criminality involved. This is not the case. Additionally, reporters sometimes seek 'consent' where they have been unable to complete customer due diligence. The process of obtaining consent is not a substitute for taking a risk based approach or for fulfilling other regulatory and legal responsibilities. The consent simply provides a person with a defence against the TF Offences, and they may still be in breach of other legal obligations by proceeding with a transaction notwithstanding that they have obtained consent. For this reason, and to avoid confusion, 'consent' for the purposes of these defences is instead referred to as a Defence Against Terrorist Financing ('DATF'). Please see the section 'How to request a Defence Against Terrorist Financing' below for information on how to request a DATF.

Under the Counter-Terrorism Act

The Counter-Terrorism Act enables the Minister with responsibility for finance to impose targeted countermeasures against designated countries, territories, governments, natural or corporate persons connected with ML, TF or proliferation financing (PF). It also creates an offence of failing to comply with an applicable direction from the Minister. For more information, see the "Targeted counter-measures" section of this guidance (section 2.1.4).

Under the Terrorist Asset-Freezing Regulations

The Terrorist Asset-Freezing Regulations define several finance offences that apply when dealing with persons designated by the Minister. It also creates several offences for dealings with such persons. For more information, see the "Targeted counter-measures" section of this guidance (section 2.1.4).

2.1.3 Reporting obligations and tipping off

Part 4 of the Terrorism Act also sets out the reporting obligations on those who believe or suspect that another person has committed (or in some cases, has attempted to commit) a TF offence. The law only places reporting obligations on individuals who come into contact with information in the course of their employment, trade, profession or business. Crucially, it distinguishes between those who are in the "regulated sector" and those who are not. The "regulated sector" for these purposes is defined in Schedule 2 of the Act. A copy of the definition can be found in Appendix 1 of this guidance note. The reader is strongly advised to refer to this definition to determine whether or not they fall within it.

A failure to comply with a reporting obligation amounts to the commission of a criminal offence.

Non-regulated sector

The obligation for those who are not in the regulated sector (as defined in Appendix 1) to report the suspicious activity of others can be found in Section 40 of the Terrorism Act.

A person commits an offence where they:

a) believe or suspect that another person has committed one of TF offences set out in the previous section of this guidance;
b) they base their belief or suspicion on information which comes to their attention in the course of a trade, profession or business or in the course of their employment; and
c) they fail to disclose their belief or suspicion and the information on which it is based to a constable as soon as is reasonably practicable.

Those who are not in the regulated sector can submit a SAR using the manual form provided on the GFIU website. Please see the section "How to make a report", below.

A person guilty of an offence under this section shall be liable-

a) on conviction on indictment, to imprisonment for a term not exceeding 5 years, to a fine or to both; or
b) on summary conviction, to imprisonment for a term not exceeding 6 months, or to a fine not exceeding the statutory maximum or to both.

It is a defence for a person to prove that they had a reasonable excuse for not making the disclosure required under this obligation.

A legal professional adviser is not required to disclose information which he obtains in privileged circumstances or a belief or suspicion based on information which he obtains in privileged circumstances. Information is obtained by a legal adviser in privileged circumstances if it comes to him, otherwise than with a view to furthering a criminal purpose:

a) from a client or a client's representative, in connection with the provision of legal advice by the adviser to the client;
b) from a person seeking legal advice from the adviser, or from the person's representative; or
c) from any person, for the purpose of actual or contemplated legal proceedings.

A person making a disclosure under this section is deemed in law to have permission to do so notwithstanding any restriction on the disclosure of such information that may be imposed by statute, contract or otherwise.

Regulated sector

The obligation for those who are in the regulated sector (as defined in Appendix 1) to report the suspicious activity of others can be found in Section 46 of the Terrorism Act.

A person commits an offence where:

a) they know or suspect or have reasonable grounds for knowing or suspecting that another person has committed or attempted to commit a TF Offence
b) the information or other matter on which their knowledge or suspicion is based or which gives reasonable grounds for such knowledge or suspicion came to them in the course of a business in the regulated sector; and
c) they fail to disclose the information to a police officer or nominated officer as soon as practicable.

The reference to a police officer above includes a reference to the police officers and custom officers in the GFIU. This obligation can therefore be complied with by submitting a report to the GFIU. Please see the section “How to make a report”, below.

This test includes an objective element. A person will be guilty for failing to report where they have reasonable grounds to believe or suspect that a TF Offence has been committed or attempted even though they did not actually hold such a belief or suspicion.

It is important to note that this test includes an obligation to report a belief or suspicion of an attempt to commit a TF Offence as opposed to just its actual committal as for non-regulated entities.

A nominated officer is a person nominated by the alleged offender’s employer to receive disclosures under this section. A disclosure to a nominated office must be made in the course of the alleged offender’s employment and in accordance with the procedure established by the employer for that purpose.

A person guilty of an offence under this section is liable-

a) on conviction on indictment, to imprisonment for a term not exceeding 5 years or to a fine or to both;
b) on summary conviction, to imprisonment for a term not exceeding 6 months or to a fine not exceeding the statutory maximum or to both.

A person does not commit an offence under this section if

a) he has a reasonable excuse for not disclosing the information or other matter;
b) he is a professional legal adviser or relevant professional adviser and the information or other matter came to him in privileged circumstances;
c) the person is employed by, or is in partnership with, a professional legal adviser or relevant professional adviser to provide the adviser with assistance or support, the information or other matter comes to the person in connection with the provision of such assistance or support and the information or other matter came to the adviser in privileged circumstances.

Information or other matter comes to a professional legal adviser or relevant professional adviser in privileged circumstances if it is communicated or given to him-

a) by (or by a representative of) a client of his in connection with the giving by the adviser of legal advice to the client;
b) by (or by a representative of) a person seeking legal advice from the adviser; or
c) by a person in connection with legal proceedings or contemplated legal proceedings

but which is not communicated or given with a view to furthering a criminal purpose.

In deciding whether a person committed an offence under this section the court must consider whether they followed any relevant guidance which was at the time concerned-

a) issued by a supervisory authority or any other appropriate body; and
b) published in a manner appropriate to bring the guidance to the attention of persons likely to be affected by it.

A disclosure made under this section shall not be taken to breach any restriction on the disclosure of information (however imposed) provided that the disclosure is made to a police officer or a nominated officer as soon as is practicable after the information or other matter comes to the discloser.

A disclosure to a nominated officer is a disclosure which–

a) is made to a person nominated by the discloser's employer to receive disclosures under this section; and
b) is made in the course of the discloser's employment and in accordance with the procedure established by the employer for the purpose.

Under the Terrorist Asset-Freezing Regulations

The Terrorist Asset-Freezing Regulations enable the minister to designate a person that he believes is or has been involved in terrorist activity, or is owned or controlled directly or indirectly by such a person, or is acting on behalf of or at the direction of such a person. The regulations also establish several offences that apply when dealing with designated persons. Whilst the offences apply to all persons, "relevant institutions" only are under an additional obligation to inform the Minister as soon as practicable if they know or have reasonable cause to suspect that a person is a designated person or has committed an offence under Part III. For more information, see the "Targeted counter-measures" section of this guidance.

How to make a report

GFIU uses a Suspicious Activity Reporting (SARs) online system (Themis) that allows for reporting entities in Gibraltar to submit SARs in a secure and digital format via a web based portal. Themis is now the preferred and recommended method for the reporting of activity suspected to be associated with TF. Reporting entities with terrorist financing reporting obligations under the Terrorism Act 2018 will be requested to register their Money Laundering Reporting Officers (MLROs), nominated persons or other with GFIU so that access can be authorised.

For direct access to Themis please visit this link.

To register with Themis as a New User requires the user to submit a registration form, which can be obtained here.

A separate signed form is required for each organisation and/or individual user being registered that are obliged to report suspicion to the GFIU. The organisation should only nominate Money Laundering Reporting Officers, Deputy MLROs, Compliance Officers and/or Directors (or equivalent) to report on their behalf. Forms must be signed by an authorised signatory. Scanned copies of the signed form will be accepted.

Manual SARs will be accepted in special circumstances or from persons that are not in the regulated sector and can be downloaded here.

Please note that it is the user's responsibility to adhere to the Themis User Manual and best practices provided with the log in credentials to ensure the integrity and security of the system. GFIU has produced a detailed guidance note on submitting SARS which can be found here.

How to request a Defence Against Terrorist Financing

Reporters wishing to obtain a DATF must do so via the Themis portal under the Consent tab. A DATF can also be requested after the SAR is submitted with no requirement to create a new SAR. For more detailed information on requesting a DATF via Themis please refer to the Themis user manual.

Please note that, unlike with a Defence Against Money Laundering (DAML), consent cannot be implied and is only deemed to be given if done so expressly. Therefore, the

lack of a response to a request can never be taken as implied consent for the purposes of obtaining a DATF.

Tipping off offence

The Terrorism Act creates a tipping off offence that only applies to persons in the regulated sector

Section	Applies to	Particulars
Section 49 - tipping off	Information coming to a person in the course of a business that is in the regulated sector.	A person commits an offence if they disclose to another party the fact that they or someone else made a disclosure of information, that disclosure is likely to prejudice any investigation that might be conducted following the disclosure, and the information on which the disclosure is based came to the person in the course of a business in the regulated sector. A person also commits an offence if they disclose that an investigation into allegations that a TF offence has been committed, is being contemplated or is being carried out and that disclosure is likely to prejudice that investigation and the information on which it is based came to them in the course of a business in the regulated sector.

2.1.4 Targeted counter-measures

Under the Terrorism Act

The Terrorism Act empowers the Minister for Justice to make freezing orders, which prohibit persons from making funds available to or for the benefit of a person or persons specified in them.

A freezing order made by the minister ceases to have effect at the end of the period of 2 years starting with the day on which it is made.

Under the Counter-Terrorism Act

The Counter-Terrorism Act enables the Minister with responsibility for finance to impose targeted countermeasures against designated countries, territories, governments, natural or corporate persons connected with ML, TF or proliferation financing (PF). The countermeasures can require one or more or all persons operating in the financial sector to take specific or general measures with regards to enhanced customer due diligence, enhanced ongoing monitoring and systematic reporting, and can ultimately require relevant persons to limit or cease business with the designated entity.

All directions by the minister under this act shall be published in the gazette. Where a direction is addressed to a particular person, a copy of the direction will also be sent

directly to them. A person who fails to comply with a requirement imposed by a direction commits an offence and is liable:

a) on summary conviction to imprisonment for 12 months or to a fine at level 5 on the standard scale or both;
b) on conviction on indictment to imprisonment for 2 years or a fine, or both.

Persons operating in the financial sector (as defined in section 5 of the Counter-Terrorism Act) should therefore establish systems to ensure they are aware of and able to comply with all directions issued under this act. However, no offence is committed if the person took all reasonable steps and exercised all due diligence to ensure that the requirement would be complied with. In deciding whether a person has committed an offence under this section the court must consider whether the person followed any relevant guidance that was at the time issued by the Minister or a supervisory authority.

An offence under this Act may be committed by a person operating in the financial sector by conduct wholly or partly outside Gibraltar. Where such an offence is committed by a body corporate and it is shown to have been committed with the consent or the connivance of an officer of the body corporate or to be attributable to any neglect on the part of any such officer, then the officer is also guilty of the offence

Under the Terrorist Asset-Freezing Regulations

The Terrorist Asset-Freezing Regulations enable the minister to designate a person that he believes is or has been involved in terrorist activity, or is owned or controlled directly or indirectly by such a person, or is acting on behalf of or at the direction of such a person. The regulations also establish several offences that apply when dealing with designated persons.

TF Offence	Particulars
Section 16 - Freezing of funds and economic resources	A person commits an offence if they deal with funds or economic resources owned, held or controlled by a designated person if they know, or have reasonable cause to suspect, that they are dealing with such funds or economic resources.
Section 17 - Making funds or financial services available to a designated person	A person commits an offence if they make funds or financial services available directly or indirectly to a designated person if he knows, or has reasonable cause to suspect, that he is making the funds or financial services so available.
Section 18 - Making funds or financial services available for benefit of a designated person	A person commits an offence if they make funds or financial services available to any person for the benefit of a designated person if he knows, or has reasonable cause to suspect, that he is making the funds or financial services so available.
Section 19 - Making economic resources	A person commits an offence if they make economic resources available directly or indirectly to a designated person if they know, or have reasonable cause to suspect that they are making the

available to a designated person	economic resources so available and that the designated person would be likely to exchange the economic resources, or use them in exchange, for funds, goods or services.
Section 20 - Making economic resources available for the benefit of a designated person	A person commits an offence if they make economic resources available to any person for the benefit of a designated person if they know, or have reasonable cause to suspect, that they are making the economic resources so available.

"funds" means financial assets and benefits of every kind, including (but not limited to)−

a) cash, cheques, claims on money, drafts, money orders and other payment instruments;
b) deposits with relevant institutions or other persons, balances on accounts, debts and debt obligations;
c) publicly and privately traded securities and debt instruments, including stocks and shares, certificates representing securities, bonds, notes, warrants, debentures and derivative products;
d) interest, dividends and other income on or value accruing from or generated by assets;
e) credit, rights of set-off, guarantees, performance bonds and other financial commitments;
f) letters of credit, bills of lading and bills of sale;
g) documents providing evidence of an interest in funds or financial resources;
h) any other instrument of export financing.

"Economic resources" means assets of every kind whether tangible or intangible, movable or immovable, which are not funds but can be used to obtain funds, goods or services.

The above offences apply to all persons. However, "Relevant institutions" are under an additional obligation to inform the Minister as soon as practicable if they know or have reasonable cause to suspect that a person is a designated person or has committed an offence under Part III.

A "Relevant institution" means−

a) a person licensed or authorised under the Financial Services (Investment and Fiduciary Services) Act 1989 or the Financial Services (Banking Act) 1992 to carry on regulated activity;
b) an undertaking that by way of business−
    i. operates a currency exchange office;
    ii. transmits money (or any representation of monetary value) by any means; or
    iii. cashes cheques that are made payable to customers.
c) a designated non-financial business or profession as defined by the FATF and not otherwise covered by these Regulations.

2.1.5 Domestic sanctions

The Sanctions Act empowers the Chief Minister to impose domestic sanctions where doing so would further the prevention of (amongst other things) terrorism or the financing of terrorism. Such sanctions may include financial sanctions, which can impose prohibitions or requirements for the purposes of freezing funds or economic resources owned held or controlled by, or preventing financial services from being provided to or procured from, or preventing funds of economic resources from being made available to or received from designated persons.

Sanctions imposed under the Sanctions Act may also grant special powers to an 'appropriate body' or require certain persons to provide information and/or documents to such a body about prescribed matters. For these purposes, an appropriate body means the Chief Minister or such other person as may be prescribed in the sanction.

It is also important to note that you may have concurrent obligations under two pieces of legislation. For example, you may be obliged to provide certain information or documents under a sanction whilst also being obliged to submit a SAR under the Terrorism Act. If this is the case, you must comply with both requirements as compliance with one does not discharge your obligation under the other.

GFIU has issued a separate and detailed guidance note dedicated to sanctions under the Sanctions Act. This can be found here.

2.2 International Obligations

2.2.1 International sanctions

The Sanctions Act 2019 also gives effect in Gibraltar to international sanctions, which include restrictive measures imposed by:

1. the United Nations Security Council;
2. the European Union;
3. the United Kingdom (acting under either the Terrorist Asset-Freezing etc Act 2010 or the Sanctions and Anti-Money Laundering Act 2018 of the United Kingdom).

Persons carrying out relevant financial business must have policies, controls and procedures which ensure that they are aware of the lists of persons to whom international sanctions apply, and ensure they undertake appropriate checks of the lists when undertaking relevant financial business and undertake action including, where appropriate, the making of disclosures to GFIU and the freezing of relevant assets.

A relevant financial business for the purposes of the Sanctions Act 2019 is any business that falls within the same definition for POCA, on which see section 2.1.1 above.

Breaching an international sanction or the requirements set out in the previous paragraph constitutes a criminal offence.

Links to the relevant lists can also be found on GFIU's website.

A consolidated list of designated persons subject to financial sanctions under UK law, as well as those subject to UN sanctions. This can be found here.

Note that the above list may include UK sanctions imposed under the Counter Terrorism Act 2008 and the Anti-Terrorism, Crime and Security Act 2001 of the United Kingdom, which are not automatically applicable in Gibraltar.

You can also subscribe to a mailing list to receive updated lists via email. You must first register an account with: https://webgate.ec.europa.eu/.

GFIU has issued a separate guidance note that is dedicated to sanctions under the Sanctions Act. This can be found here.

3 Jurisdictional terrorist financing risk in Gibraltar

Gibraltar's most recent national risk assessment was published in August 2020. Whilst the TF risk at a jurisdictional level has been assessed as low, the risk may increase in specific sectors of the economy or when dealing with higher risk jurisdictions. This chapter deals with the TF risks faced by Gibraltar at the jurisdictional level, drawing on key findings from the NRA, whilst sector-specific guidance on TF risks are dealt with in chapter 4.

3.1 Overview

Gibraltar is a small finance centre which is largely UK customer facing in financial services and on-line gambling. Traditional financial services products for Gibraltar had been the provision and servicing of corporate structures and private banking. Over the last two decades these services have been in decline and replaced with on-line gambling, e-money products and more recently, distributed ledger technologies.

Gibraltar's geographic and demographic characteristics are such that it is less likely to be a jurisdiction in which terrorists raise funds or spend them for the purposes of carrying out an attack. Whilst such a possibility cannot be excluded, Gibraltar's main TF risk arises from its high levels of cross border business involving the movement of funds, which can manifest itself in one or more of the following ways:

1. Flow-through, whereby Gibraltar is used as a transit country for funds intended for use in foreign terrorism;

2. Service provision, whereby terrorist funds do not enter Gibraltar but where businesses in Gibraltar provide administration or other services to parties that support foreign terrorism, including internationally active domestic or foreign entities, politically exposed persons (PEPS) or high net worth individuals;

3. The use of complex structures involving legal persons and legal arrangements to disguise the underlying beneficial owner who may be involved in terrorism or TF or feature on a terrorism related sanctions list;

4. Abuse of NPOs, whereby donations or aid that are sent to or administered from Gibraltar go to conflict zone or other high risk jurisdictions and are diverted to support foreign terrorism;

At present there is little evidence to suggest that Gibraltar is being used to channel terrorist funds, however this does not obviate the need to remain aware of the threat and vulnerabilities faced by the jurisdiction. A crucial factor when considering the TF threat faced is the extent of any connection between Gibraltar and conflict zones or other high risk jurisdictions. This is considered in section 3.2. It is also important to appreciate the extent to which terrorism or TF is occurring in jurisdictions with which Gibraltar has close geographic and/or political links. This is done in section 3.3. Individual operators will need to consider the same at the organisational level when conducting their own risk assessments.

3.2 Links with conflict zones and high risk jurisdictions

3.2.1 Conflict zones

A 'conflict zone' includes:

1. jurisdictions/regions that are unstable, at war, where armed hostility is present or where terrorist organizations are active.
2. Provinces/regions with known links to terrorist organizations or share a border with territories controlled by terrorist organizations.
3. Countries where funds and other assets are generated (e.g., originator of the funds transfer) for terrorism acts or terrorist organizations irrespective of where those acts take place or organizations reside.
4. Jurisdictions/regions that are transit points or have had money flows to/from known foreign-terrorist fighters (FTFs).

Transactions and business relationships with conflict zones are particularly susceptible to TF risks. There have been numerous cases of TF facilitators located in jurisdictions neighbouring a conflict to assist in transporting funds and other goods (including foreign terrorist fighters) into or out of conflict zones.

Although Gibraltar is not itself close to a conflict zone the assessment conducted by the FSC on the inflows and outflows of funds by the financial services industry has identified some transactions received from and issued to such jurisdictions.

E-money products were the most widely used products in these conflict zone jurisdictions, however, the average value of the transactions are low. Banking transactions with these jurisdictions, whilst fewer in number, are generally of a higher value. This is to be expected given that the banking system is generally used to transfer larger amounts of money than e-money, in which the sums tend to be very low and related to individual or personal expenses.

Operators must be extremely cautious when transacting with entities that are based in or linked to these countries.

3.2.2 High risk jurisdictions

There is no single definition of a high risk jurisdiction, but they can include:

1. Countries/areas identified by credible sources as providing funding or support for terrorist activities or that have designated terrorist organisations operating within them;
2. Countries identified by credible sources as having significant levels of organised crime, corruption, or other criminal activity, including being a major source or a major transit country for illegal drugs, human trafficking and smuggling and illegal gambling;
3. Countries subject to sanctions, embargoes or similar measures issued by international organisations such as the United Nations;
4. Countries identified by credible sources as having weak governance, law enforcement, and regulatory regimes, including countries identified by FATF

statements as having weak AML/CFT regimes, in relation to which financial institutions (as well as DNFBPs) should give special attention to business relationships and transactions;

5. Countries identified by credible sources to be uncooperative in providing beneficial ownership information to competent authorities, a determination of which may be established from reviewing FATF mutual evaluation reports or reports by organisations that also consider various co-operation levels such as the OECD Global Forum reports on compliance with international tax transparency standards.

The FATF maintain a list of monitored countries (http://www.fatf-gafi.org/countries/#high-risk).

As with conflict zones, transactions and business relationships with high-risk jurisdictions are particularly susceptible to TF risks. Fortunately, Gibraltar's customer base in financial services is only marginally derived from FATF high risk jurisdictions.

Operators must be extremely cautious when transacting with entities that are based in or linked to high risk jurisdictions.

3.3 Geographic & Political link

3.3.1 Spain

Gibraltar needs to be aware of the TF risks present in Spain given she is our closest neighbour with whom daily trade is conducted across all sectors of the economy. The most recent FATF follow-up report is to be found here.

It notes that:

1. Spain continues to face a high risk of TF from Jihadist terrorist groups, including a slight increase in the risks of returning foreign terrorist fighters.
2. The risk of radicalised individuals supporting terrorist organisations by providing funds, including through the misuse of MVTS providers, remains to be among the key challenges for the competent authorities of Spain.
3. Some types of NPOs continue to be vulnerable to TF abuse as well.

The TF risk posed to Gibraltar by Spain has been assessed in the NRA as being **high**.

3.3.1 Morocco

Morocco needs to be accounted for in terms of a jurisdictional risk assessment given its close proximity to Gibraltar. Morocco is one of the leading cannabis producers in the world, supplying most of Europe's demand for the product. Although Gibraltar sits between long established drug trafficking routes, it is not a destination point but OCGs on both sides of the Strait can exploit these trafficking routes for migrant smuggling. With the increase in radicalisation in northern Africa and the Sahel, there is a corresponding increase in the threat of terrorist activity, and therefore TF risk that arises from migration of persons from these regions.

Morocco's latest mutual evaluation report was published in April 2019. It notes that:

> *"Terrorism and its financing still pose a serious threat to Morocco despite the significant efforts exerted by competent authorities in combating terrorism; this threat mainly stems from Moroccan FTFs whose number is estimated to be around 1600. In addition to the risks resulting from terrorist organizations, such as Daesh and threats related to Al-Qaida, mainly its branch known as "Al-Qaida in the Islamic Maghreb", despite their declining activity following the emergence of the terrorist organization Daesh, as well as the threats posed by the terrorist group "Islamic Movement of the Levant".*

There are no known links between OCGs operating in the area and TOs. However, given TOs tend to engage in or be funded by criminal activities, the possibility that the North African element of the OCG operations are supporting TOs can't be excluded.

The TF risk posed to Gibraltar by Morocco has been assessed in the NRA as being **high**.

3.3.1 United Kingdom

Whilst the United Kingdom may be some distance away, Gibraltar's close political and economic links with it warrants giving it individual consideration. Their most recent mutual evaluation report notes:

> *"The UK faces severe threats from international terrorism. Terrorist financing activity in the UK is usually low-level, involving small amounts of funds raised by UK based individuals to fund their own travel to join terrorist groups, to send to terrorist associates, or to finance their own terrorist attack plans. The UK also faces threats from Northern Ireland-related terrorism which are rated severe in Northern Ireland and substantial in Great Britain. The nature of the Northern Ireland-related terrorism threat has evolved with paramilitaries and terrorist groups focusing on forms of organised crime which are not all specifically intended to raise funds for terrorism."*

3.4 Demographic factors

Terrorist financiers have been known to utilise local diaspora communities, and their ethnic links and family ties to raise and move funds and other assets to support terrorist activities. The potential for sympathetic views to be held by local members of the community increases where there are strong communal links to areas with an active terrorist threat. The economic activity flowing between the community (for example through family support remittances) terrorist activity may be used to conceal TF. Fortunately, Gibraltar does not have a local diaspora community and the only link to another community is to the population of Moroccan origin, which is well integrated.

3.5 Likelihood of a terrorist attack in Gibraltar

Whilst there has not been an actual terrorist attack in Gibraltar, such an attack can't be ruled out in light of the heightened threat globally against UK interests and British nationals from groups or individuals motivated by the conflict in Iraq and Syria. There therefore remains the possibility that a small cell, lone actor or TO may move funds into Gibraltar with a view to using them to fund a local attack.

Threat levels are designed to give a broad indication of the likelihood of a terrorist attack. For further information on Gibraltar's threat level visit the Royal Gibraltar Police website.

3.6 Abuse of Non-Profit Organisations

NPOs are a vibrant and integral part of the contemporary global environment and play a significant role in combatting terrorism. However, organisations and individuals have in the past taken advantage of the NPO sector to support those who engage in terrorism or support to terrorist organisations.

Case Study: Exploitation of a legitimate charity

A suspicious transaction report (STR) was made following an attempt by Individual A, to deposit substantial amounts of cash into the account of a charity – over which he had power-of-attorney – with the instruction that it be transferred onward to a notary as an advance for the purchase of real estate. The Investigation revealed that:

- Payments into the account consisted of multiple cash deposits (presumably donations) but also payments directly from the account of Individual A. In turn, A's personal account revealed multiple cash deposits that corresponded to donations from private individuals.
- The debit transactions consisted of transfers to the non-profit organisation (NPO) and international transfers to Individual B. Police sources revealed that A had links with individuals that were known for terrorist activities, including B.
- Law enforcement assessed that the charity, which continued to fulfil an important social function, was being exploited both as a "front' to raise funds and as a "means of transmission" to divert a portion of them to known terrorist associates of A.

Commentary: This case is indicative of the vulnerabilities to exploitation that arise with weak governance combined with high levels of cash deposits.

Source: FATF Terrorist Financing Typologies Report 2015

Abuse of NPOs can involve diverting legitimate donations through affiliated individuals to TOs, creating false or sham NPOs to obtain funding from unwitting donors, abusing a NPO's program implementation to aid the TO, supporting recruitment into TOs and exploiting NPO authorities. NPOs most at threat are:

1. Those engaged in service activities which operate in close proximity to an active terrorist threat; and
2. 'correspondent' NPOs, which send funds to them that have been raised from other regions.

Case Study: Diversion of funds collected by a charity

A client was receiving donations/small amounts of money from different people located in Germany in his account in Switzerland. He informed the bank that he could not open an account for his charity in Germany due to legal restrictions and so he was using his private Swiss banking account for collecting donations. The donations were meant to be withdrawn in cash and brought personally to Tanzania to build a fountain. According to the bank statements different reasons were declared by the donators: "Donation Africa Fountain", "Donation Streetwork", "Tansania Orphanage", "Mosque Building", "Koran School" etc. Media reported that the NPO "Africa Fountain" was close to extremists related to terrorism.

Source: FATF Emerging Terrorist Financing Risks 2015

Gibraltar's NPO sector is large and varied with nearly 300 registered charities and a dozen Friendly Societies. Many are small charities used for single purposes or causes. Others have a wider scope and serve both the local community as well as specific projects outside of Gibraltar. Some of these charities, however, are relatively large and may present a higher TF risk. In the analysis of the NPO sector undertaken in 2017, data as to inflows and outflows of donations and charitable work showed that most charitable donations were from Gibraltar itself followed by the UK, Switzerland and Israel. The charities' work, however, were based mainly in Israel, UK, and Gibraltar. When analysed further the results of the donation base and the activity of the charity are commensurate with the activities of the locally based charities which are either offshoot or UK based charities or where substantial educational grants are provided.

The overall risk in Gibraltar of abuse of NPOs for terrorist purposes has been assessed as **low**.

Case Study: Possible links between FTFs and a charitable foundation

Netherlands noticed that some stichtingen (foundations) and NGO's, working in the field of e.g., charity and religion, could be linked to FTFs. As of yet there is no hard evidence of TF, but involvement of FTFs in the periphery of these legal entities has been established, and people associated with the foundations have been found to travel to Syria with large amounts of cash. Donations were received from foreign countries, and then transferred through bank accounts of foundations that did not share similar goals or activities but were chaired by or related to the same individual. Money was eventually withdrawn from bank accounts, which made it hard to trace its end-use.

Source: FATF Emerging Terrorist Financing Risks 2015

For more information, please see the NCO's newsletter on NPOs, which can be found here.

4 Sector specific threats and terrorist financing typologies

There are no confirmed TF incidents in Gibraltar. However, the absence of known cases does not necessarily mean that there is a low risk. It is therefore important for operators to remain vigilant and continually monitor their TF exposure. For most sectors, the applicable regulatory regime will have gone a long way to addressing the vulnerabilities to a given threat, thereby reducing the overall risk posed. Nevertheless, no regulatory regime is capable of extinguishing all TF risk. This is especially so given that the sums involved in TF are usually much lower than for ML and terrorists and their financiers or sympathisers may be legal citizens who are as of yet unknown to any terrorist lists. They are therefore often able to proffer seemingly legitimate explanations for their activity and pass CDD checks, thereby making TF activity extremely difficult to detect. Operators must therefore fully understand the nature of the TF threat they face through analysis of its known typologies and case studies so as to minimise the chances of any cases going undetected.

This section aims to provide sector-specific guidance on the TF threats faced by various sectors of the economy. It draws on the recently published National Risk Assessment as well as various reports produced by FATF. The reader is advised to read the National Risk Assessment for the full assessment on the risk to a given sector. This guidance does not seek to re-address the assessment of risk as set out in the NRA, but rather supplement the NRA with known typologies, case studies and risk indicators where they are available.

It is important to note that operators will rarely be able to detect TF as such given the difficulties outlined above. Where funds are derived from criminal activity, then traditional monitoring mechanisms that are used to identify money laundering may also be appropriate for TF, though the activity, which may be indicative of suspicion, may not be identified as or connected to TF. Indeed, the only time that an operator might clearly identify TF as distinct from other criminal misuse is when a known terrorist or TO has opened an account. Operators are, however, in a position to detect suspicious transactions that, if reported, may, upon further investigation by the competent authorities, prove to be related to terrorist financing. It is the competent authorities who are then in a position to determine whether the transaction relates to a particular type of criminal or terrorist activity and decide on a course of action. For this reason, it is not the responsibility of operators to conclusively determine the type of underlying criminal activity or the intended terrorist purpose. Instead, they should simply decide whether transactions are unusual, suspicious or otherwise indicative of criminal or terrorist activity and make the necessary report.

Risk indicators are therefore provided where possible to assist in suspicious activity monitoring and reporting systems. Certain risk indicators are confidential in nature. These will be provided by GFIU directly to the relevant operators. Where risk indicators are provided, they should not be considered exhaustive and nor should they be slavishly relied on as a substitute to adopting a fully risk-based approach. It is important to note that a single indicator may not alone warrant suspicion of TF or provide clear indication of such activity. These cases could instead simply warrant further monitoring and examination. Similarly, the existence of several indicators may warrant further examination before reasonably giving rise to a suspicion of TF.

All operators across all sectors must be particularly cautious where a transaction in question is linked with a conflict zone or high risk jurisdiction.

4.1 E-money / Prepaid cards

"Electronic money" means electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions and which is accepted by a natural or legal person other than the electronic money issuer. A key characteristic of e-money is its prepaid nature. This means that an account, card or a device needs to be credited with a monetary value for that value to constitute e-money.

The majority of SARs submitted to the GFIU were based on perceived inadequate due diligence and/or failure to provide due diligence by individual customers. SARs based on the suspicion of fraud, false accounting and/or forgery are also frequently submitted.

4.1.1 Transporting value to conflict zones or high risk jurisdictions

Prepaid cards present an advantage over cash in that they are a more secure way of moving money to high-risk jurisdictions or conflict zones. This is due to the logistical benefits of transporting a discreet number of prepaid cards rather than physical cash and the reduced risk of theft whilst in transit. Once in a high-risk jurisdiction or conflict zone, the cards can be used to withdraw funds across several ATMs which can then be spent towards terrorist purposes.

Once in their target country, it is less likely prepaid cards will be used as a direct payment instrument due to their reduced acceptance as a form of payment and their increased traceability as compared with cash. The primary TF risk is therefore that a card is loaded with funds and transported to a high-risk jurisdiction or conflict zone to be withdrawn in multiple ATM transactions, or sold to a third party for cash at a discount. Where peer-to-peer transfers are allowed, there is also the risk that two card holders could be working in concert. This would entail one cardholder loading his card with funds raised in country A and transferring them to another cardholder who withdraws them in a conflict zone or high risk jurisdiction.

Case Study: Possible use of prepaid cards for terrorist financing purposes

In a particular case, a father and his son, suspected to be operating as money remitters, held numerous prepaid cards which were charged daily from all over Italy. Shortly after, the sums were withdrawn so as the cards accounts' balances were almost always near to zero. A portion of the sums withdrawn from the prepaid cards was transferred to a bank account held by the father; funds were also credited to the same bank account from Pakistanis. The funds on the account were further used to order credit transfers. Both persons were found to be involved in the terrorist attacks which occurred in Mumbai in 2008.

Source: FATF Money Laundering using New Payment Methods 2010

4.1.2 Use for domestic attacks and travelling foreign terrorist fighters

The risk that prepaid cards will be used as a payment instrument for terrorist purposes is higher when considering domestic terrorists and FTFs on route to conflict zones.

Case Study: Possible use of prepaid cards for FTFs

A MLRO submitted a SAR concerning two accounts registered in Turkey. The account holders used a similar pattern in their e-mail and lived at the same address, however the IP Addresses were different. Accounts had travel related transactions (flight / hotel). Further, the cards were being purchased from the same locations.

The MLRO suspected that the cards/transactions could be used to facilitate the movement of individuals into Turkey for potential terrorist activity. The Subjects were based in the UK and had no financial footprints in / ties to Gibraltar. The business relationship was terminated and the GFIU disseminated information to the relevant jurisdictions.

Source: Gibraltar Financial Intelligence Unit

A small cell / lone actor may use prepaid cards to pay for the preparatory steps for an attack in Europe, with little regard for whether they survive or escape arrest. Such was the case in the Paris attacks of 2015.

4.1.3 Open loop (cash purchasing)

Risk level: high

Loop cards are prepaid cards which can be used at any retailer or merchant as well as well as, in some cases, ATMs. The TF risk posed by open loop prepaid cards is increased by allowing cash funding, especially for 'anonymous' cards where the level of funds involved are below the CDD thresholds. Gibraltar-based EMIs are not permitted to offer such cards and the lower CDD thresholds placed by the 5th Anti-Money Laundering Directive in response to the Brussels and Paris attacks helps to reduce the TF risk across Europe generally.

4.1.4 Open loop (linked to a bank account)

Risk level: medium

The terrorist financing inherent risk for non-cash-based e-money products can be considered similar to that for other banking products or credit cards. Despite the origins of funds being known and traceability of payments being complete, perpetrators can use these products as a means of payment even if they have to pass customer due diligence measures. This is because most of the time perpetrators are unknown entities that will not be on sanctions lists or flagged in background checks.

4.1.5 Closed loop

Risk Level: low

Closed loop cards can only be used to purchase goods and services within a single network or limited network of service providers. They present a lower risk because they are not accepted outside of their network and usually do not allow their value to be redeemed in cash. However, there are known cases of closed loop cards being used as an intermediate store of value.

Case Study: Social network fundraising with prepaid card

Individuals associated with ISIL called for donations via Twitter and asked the donors to contact them through Skype. Once on Skype, those individuals asked donors to buy an international prepaid card (a credit for mobile phone or the purchase of an Apple or other programs or credit for playing on the Internet) and send them the number of this prepaid card via Skype. Then, the fundraiser sent this card number to one of his followers in a neighbouring country from Syria, who would sell this card number at a lower price and give the cash proceeds to ISIL.

Source: FATF Emerging Terrorist Financing Risks 2015

Case Study: Suspected use of a closed-loop card company for money laundering and terrorist financing

Law enforcement information indicated that the owner of a prepaid phone card company was suspected of money laundering and having links to a terrorist organisation. The owner conducted many large cash deposits into personal and business bank accounts and when questioned would indicate that prepaid phone cards were sold to retailers and convenience stores, and cash payments were received instead of cheques. This was apparently due to the fact that the owner was not confident that cheques would be honoured. Some of the deposits were also conducted into accounts held by prepaid phone card suppliers. Electronic funds transfers were also ordered by the owner to the benefit of individuals in Europe and the Middle East, sometimes through accounts which previously had not seen much activity. The owner was also the beneficiary of funds ordered by the same individuals.

Source: FATF Money Laundering using New Payment Methods 2010

4.1.6 Risk indicators

1. Discrepancies between the information submitted by the customer and information detected by monitoring systems
2. Individuals who hold an unusual volume of prepaid card accounts with the same provider
3. A large and diverse source of funds (i.e., bank transfers, credit card and cash funding from different locations) used to fund the same account(s)

4. Multiple reference bank accounts from banks located in various cities used to fund the same account
5. Loading or funding of account always done by third parties
6. Numerous cash loading, just under the reporting threshold (i.e., structured loading of prepaid cards), of the same prepaid card(s), conducted by the same individual(s) on a number of occasions
7. Multiple third party funding activities of an account, followed by the immediate transfer of funds to unrelated bank account(s)
8. Multiple loading or funding of the same accounts, followed by ATM withdrawals shortly afterwards, over a short period of time
9. Multiple withdrawals conducted at different ATMs (sometimes located in various countries different from jurisdiction where account was funded)
10. Account only used for withdrawals, and not for POS or online purchases
11. Atypical use of the payment product (including unexpected and frequent cross-border access or transactions)
12. unexplained business rationale which could be suspicious

Other, confidential risk indicators will be provided by the GFIU to licensed e-money institutions directly.

4.2 Banking

4.2.1 Deposit taking

Risk Level: medium

Terrorists, as well as their supporters or facilitators could potentially place funds from legitimate or criminal sources into the financial system with a view to using them for terrorist purposes. International experience shows that terrorist groups frequently use deposits on account to enter cash in bank accounts and withdraw money for terrorist activities, however some basic knowledge and planning capabilities are required on their part to ensure the funds appear legitimate. Banks continue to be exposed to TF risks and deposits on account represent one of the easiest ways to introduce money into the financial system. The risk of exposure is even greater where the origin of funds is legitimate, such as employment or legitimate businesses, as it becomes harder to distinguish these with legitimate activity.

Case Study: Diversion of funds from legitimate business

The personal bank account of Person A (a restaurant manager) regularly received cheques drawn from wooden pallet Company B, as well as significant cash deposits. The account did not show any 'normal' financial activity such as payment for food, travel, etc.

The bank account of Company B also showed significant cash withdrawals of between EUR 500000 and EUR 1 million. The bank where A's account was held became suspicious because of the inconsistency between Person A's profession and the nature of Company B's business and submitted a suspicious transaction report to the financial

intelligence unit. FIU analysis revealed that the individuals concerned were linked to Salafist movements, and the case was referred to prosecutors for wider investigation.

Source: FATF Terrorist Financing Typologies Report 2008

Although the use of deposits on account may be a common approach for TF activities internationally, this has not been found to be used by individuals in Gibraltar. When it comes to sending money to conflict zones, the TF risk is lower in deposits on accounts as perpetrators prefer the use of other products such as MVTS or E-money products. Notwithstanding the above, banks must remain vigilant to the possibility that account holders may seek to deposit funds with the ultimate aim of transferring them to a TO or withdrawing funds with a view to spending them for terrorist purposes.

Case Study: Use of deposit account for TF under the guise of legitimate earning

A foreign national residing in Belgium performed significant foreign exchange transactions shortly after officially establishing himself in Belgium. There was no obvious economic rationale for these transactions, which in any case were at a level that was at odds with his financial profile. An STR was submitted, which – following enquiries by judicial authorities to an exchange house – was followed by a further disclosure which indicated that funds were routed to an individual in Asia, whom police sources suspected of being part of a terrorist organisation seeking to procure weapons.

Source: FATF Terrorist Financing Typologies Report 2008

Risk Indicators[3]

1. The customer is a cash-intensive undertaking.
2. The customer is an undertaking associated with higher levels of money laundering risk, for example certain money remitters and gambling businesses.
3. The customer is an undertaking associated with a higher corruption risk, for example operating in the extractive industries or the arms trade.
4. The customer is a non-profit organisation that supports jurisdictions associated with an increased TF risk
5. The customer is a new undertaking without an adequate business profile or track record.
6. The customer is a non-resident.
7. The customer's beneficial owner cannot easily be identified, for example because the customer's ownership structure is unusual, unduly complex or opaque, or because the customer issues bearer shares.
8. The customer is reluctant to provide CDD information or appears deliberately to avoid face-to-face contact.
9. The customer's evidence of identity is in a non-standard form for no apparent reason. The customer's behaviour or transaction volume is not in line with that expected from the category of customer to which they belong, or is unexpected based on the information the customer provided at account opening.
10. The customer's behaviour is unusual, for example the customer unexpectedly and without reasonable explanation accelerates an agreed repayment schedule, by means either of lump sum repayments or early termination; deposits or demands payout of high-value bank notes without apparent reason; increases activity after a period of dormancy; or makes transactions that appear to have no economic rationale.

[3] For more information, see the European Banking Authority's consultation paper on ''The Risk Factors Guidelines''. Available at: https://www.eba.europa.eu/regulation-and-policy/anti-money-laundering-and-e-money/revised-guidelines-on-ml-tf-risk-factors

11. The customer's funds are derived from personal or business links to jurisdictions associated with higher ML/TF risk.
12. The payee is located in a jurisdiction associated with higher ML/TF risk. Firms should pay particular attention to jurisdictions known to provide funding or support for terrorist activities or where groups committing terrorist offences are known to be operating, and jurisdictions subject to financial sanctions, embargoes or measures that are related to terrorism, financing of terrorism or proliferation.

4.3 Distributed Ledger Technology (DLT)

DLT is still a nascent technology and the extent to which it will be used for TF remains to be seen. Virtual Assets (VAs) are currently one of the most popular uses of DLT. VAs are a digital representation of a value that can be traded online, and include well known digital currencies such as Bitcoin. The European Union's Supranational Risk Assessment Report shows that terrorist organisations may have an interest in utilising VAs to finance terrorist activities. The Egmont group of Financial Intelligence Units has detected cases of terrorist groups using VAs and giving instructions on social networks on how to use VAs to donate funds to terrorist causes.

Case Study: Promotion of virtual currency to fund terrorism

On 28 August 2015 Ali Shukri Amin was sentenced to 11 years in prison to be followed by a lifetime of supervised release and monitoring of his internet activities for conspiring to provide material support and resources to the ISIL.

Amin pleaded guilty on 11 June 2015. He admitted to using Twitter to provide advice and encouragement to ISIL and its supporters. Amin, who used the Twitter handle @Amreekiwitness, provided instructions on how to use bitcoin, a virtual currency, to mask the provision of funds to ISIL, as well as facilitation to ISIL supporters seeking to travel to Syria to fight with ISIL. Additionally, Amin admitted that he facilitated travel for a Virginia teenager, who travelled to Syria to join ISIL in January 2015. This teenager, was charged on 10 June 2015, in the Eastern District of Virginia with conspiring to provide material support to terrorists, conspiring to provide material support to ISIL and conspiring to kill and injure people abroad.

Amin's Twitter account boasted over 4 000 followers and was used as a pro-ISIL platform during the course of over 7 000 tweets. Specifically, Amin used this account to conduct twitter-based conversations on ways to develop financial support for ISIL using on-line currency, such as bitcoin, and ways to establish a secure donation system or fund for ISIL. For example, Amin tweeted a link to an article he had written entitled "Bitcoin wa' Sadaqat al-Jihad" (Bitcoin and the Charity of Jihad). The article discussed how to use bitcoins and how jihadists could utilise this currency to fund their efforts. The article explained what bitcoins were, how the bitcoin system worked and suggested using Dark Wallet, a new bitcoin wallet, which keeps the user of bitcoins anonymous. The article included statements on how to set up an anonymous donations system to send money, using bitcoin, to the mujahedeen.

Source: FATF Emerging Terrorist Financing Risks 2015

Gibraltar has established a full regulatory framework for the DLT space and a KYC compliance framework for ICOs. In doing so, it has substantially mitigated the inherent

risk that the DLT space presents. Compliance with the requirements of POCA (and by doing so AMLD5 and the revised FATF standard) as well as creating barriers to entry into the regulated space Gibraltar seeks to ensure that ML and TF risks are reduced considerably. The extension of KYC processes to include transactional data like IP, MAC and other unique identifiers extends the traceability and accountability of virtual assets which transact through Gibraltar.

Risk Indicators

FATF has produced a report setting out various risk indicators for virtual assets, which is intended to assist any virtual asset service provider (VASP) in its monitoring and reporting. It can be found here.

4.3.1 Wallet providers

Risk Level: medium

Custodial wallet providers receive and store and the customer's private keys, thereby taking full custodial control of the underlying virtual asset. The threat posed by these services can be considered similar to online payment services and e-money/prepaid accounts.

Case Study: Promotion of anonymous wallets to facilitate

As early as July 2014, ISIS-affiliated individuals advocated the use of Bitcoin mixing technology to conceal the movement of funds. An individual identified as Taqiul-Deen alMunthir wrote a blog post entitled 'Bitcoin and the Charity of Violent Struggle', calling for ISIS to use services such as DarkWallet. The blog states:

> *'DarkWallet's beta release will be published within the next coming months, the mujahideen Dawlatul Islam would simply need to set up a wallet and post their addresses online. Then, Muslims from across the globe could simply copy the wallet address, login to their [wallets], purchase whatever amount of bitcoin they wish to send, and send them over'.*

This study did not identify any confirmed cases of terrorists using Bitcoin mixers. But the above quote, whilst from a lone blog post and not necessarily indicative of ISIS's broader strategic intent, at least reveals that some jihadists aspire for access to anonymous online financial transfers.

Source: Policy Department for Citizens' Rights and Constitutional Affairs, "Virtual currencies and terrorist financing: assessing the risks and evaluating responses" 2018

4.3.2 Exchanges

Risk Level: low

Exchange platforms (a person or entity engaged in the exchange of virtual asset for fiat currency, fiat currency for virtual asset, funds or other brands of virtual assets) may accept a wide range of payments, including cash, credit transfers, credit cards and other virtual assets. They include cashpoint machines. Gibraltar's DLT framework captures

conversions between fiat currencies and virtual assets and conversions from one virtual asset to another.

At present there are no known TF case studies or typologies surrounding the use of DLT exchanges. GFIU will continue to monitor this sector carefully and will update this guidance accordingly as new information becomes available.

4.4 Gambling

Risk Level: low

Gibraltar has a small and closely regulated gambling sector consisting mainly of remote gambling operators in the B2C and B2B sectors with one casino licence holder operating two small land based casino premises and two betting premises. A number of gaming machines are located in premises (such as bars and restaurants) throughout Gibraltar. None of the products in the gambling sector are considered to pose a significant TF risk. There does however exist the specific risk that terrorist financiers could use peer-to-peer transfers between users of the platform. This can occur either as transfers involved in 'staking' players or through the deliberate losing of funds (so-called "chip dumping") by one player to another.

Case Study: Customer with possible links to TF

During their CDD a gaming company came across information related to the subject having been arrested for importing counterfeit cigarettes. Further searches revealed that a person shown as a co-habitant at his address, with the same surname, was being sought for a GBP 1 billion tax fraud in Italy using fake companies.

A press release suggested that this was for the purpose of funding terrorism. The Subject was based in the UK and had no financial footprints in / ties to Gibraltar. Intelligence was disseminated to the relevant jurisdictions by the GFIU and the business relationship terminated by the gaming company.

Source: Gibraltar

Risk Indicators:

1. Information provided by the player contains a number of mismatches (e.g. email domain, telephone or postcode details do not correspond to the country);
2. The registered credit card or bank account details do not match the player's registration details;
3. The player is situated in a higher-risk jurisdiction or is identified as being listed on an international sanctions list;
4. The player is identified as a politically exposed person;
5. The player seeks to open multiple accounts under the same name;
6. The player opens several accounts under different names using the same IP address;
7. The withdrawals from the account are not commensurate with the conduct of the account,
8. such as for instance where the player makes numerous withdrawals without engaging in significant gambling activity;

9. The player deposits large amounts of funds into his online gambling account;
10. The source of funds being deposited into the account appears to be suspicious and it is not possible to verify the origin of the funds;
11. The customer logs on to the account from multiple countries;
12. A deposit of substantial funds followed by very limited activity;
13. The player has links to previously investigated accounts;
14. Different players are identified as sharing bank accounts from which deposits or withdrawals are made.

4.5 Trust and Company Services Providers

Whilst the trust and company services sector encompasses a wide range of activities, the significant TF risks in this sector come from the creation of legal entities (and other legal arrangements) and their ongoing business activities. The risk for these activities have been assessed in the National Risk Assessment as **medium**.

Firms and/or individuals who perform these functions in Gibraltar are required to be licenced and regulated as a trust and company service provider (TCSP). The POCA systems of control extend to Customer Due Diligence on the customers of the TCSPs, their beneficial owners and the identification of PEPs, their family and known close associates as well as ongoing transaction monitoring requirements. With 98% of all Gibraltar legal entities being managed through TCSPs, risks that are normally associated with legal entities (complex and opaque structures to hide beneficial owners) are substantially mitigated. The GFSC's supervisory programme includes verification that the requirements of POCA and the GFSC's AML/CFT Guidance Notes are being adhered to.

The main risk to TSCPs comes from larger terrorist organisations, which are structured more like large businesses and may use corporate and/or trust structures in the management of their assets.

Case Study: a TCSP discovers suspicious activity during on-going monitoring

A TCSP during its CDD on-going monitoring identified a payment of GBP 366 made from a personal bank account outside of Gibraltar to a charity declared by the UAE as a terrorist group. The Subject was based in the UK and had no financial footprint in Gibraltar. Intelligence was spontaneously disseminated to the relevant jurisdiction by the GFIU.

Source: Gibraltar

Risk Indicators:

Country/Geographic risk - The provision of services by a TCSP may be higher risk when features of such services are connected to a higher risk country, for example:

a) the origin, or current location of the source of funds in the trust, company or other legal entity;

b) the country of incorporation or establishment of the company or the trusts;

c) the location of the major operations or assets of the trust, company or other legal entity; and

d) the country in which any of the following is a citizen or tax resident: a settlor, beneficiary, protector or other natural person exercising effective control over the trust or any beneficial owner or natural person exercising effective control over the company or other legal entity.

Client risk - In the examples given below, the client of TCSPs may be an individual who is a settlor or beneficiary of a trust, or beneficial owner of a company, or other legal entity that is, for example, trying to obscure the real beneficial owner or natural person exercising effective control of the trust, company or other legal entity. The client may also be a representative of a company's or other legal entity's senior management who are, for example, trying to obscure the ownership structure. The key risk factors that TCSPs should consider are:

a) The TCSP's client base includes industries or sectors where opportunities for TF are particularly prevalent.

b) The client include PEPs or persons closely associated with or related to PEPs, who are considered as higher risk clients.

c) Clients conducting their business relationship or requesting services in unusual or unconventional circumstances (as evaluated taking into account all the circumstances of the client's representation).

d) Clients where the structure or nature of the entity or relationship makes it difficult to identify in a timely manner the true beneficial owner or controlling interests or clients attempting to obscure understanding of their business, ownership or the nature of their transactions, such as:

i. Unexplained use of shell and/or shelf companies, front company, legal entities with ownership through nominee shares or bearer shares, control through nominee or corporate directors, legal persons or legal arrangements splitting company incorporation and asset administration over different countries, all without any apparent legal or legitimate tax, business, economic or other reason.

ii. Unexplained use of informal arrangements such as family or close associates acting as nominee shareholders or directors without any apparent legal or legitimate tax, business, economic or other reason.

iii. Use of trust structures for tax evasion or to obscure ownership in order to place assets out of reach to avoid future liabilities.

e) Unusual complexity in control or ownership structures without a clear explanation, where there are certain transactions, structures, geographical location, international activities or other factors are not consistent with the TCSP's understanding of the client's business or economic purpose behind the establishment or administration of the trust, company or other legal entity with respect to which the TCSPs are providing services.

f) Unusually high levels of assets or unusually large transactions compared to what might reasonably be expected of clients with a similar profile may indicate that a client not otherwise seen as higher risk should be treated as such.

g) The offer by the person giving instructions to the TCSP to pay extraordinary fees for services, which would not ordinarily warrant such a premium.

h) The relationship between employee numbers/structure is divergent from the industry norm (e.g. the turnover of a company is unreasonably high considering the number of employees and assets compared to similar businesses)

i) Sudden activity from a previously dormant client without a clear explanation.

j) Clients that start or develop an enterprise with unexpected profile or abnormal business cycles or clients that enter into new/emerging markets. Organised criminality generally does not have to raise capital/debt, often making them first into a new market, especially where this market may be retail/cash intensive.

k) Indicators that client does not wish to obtain necessary governmental approvals/filings, etc.

l) Payments received from un-associated or unknown third parties and payments for fees in cash where this would not be a typical method of payment.

m) Clients who have funds that are obviously and inexplicably disproportionate to their circumstances (e.g. their age, income, occupation or wealth).

n) Clients who appear to actively and inexplicably avoid face-to-face meetings or who provide instructions intermittently without legitimate reasons and are otherwise evasive or very difficult to reach, when this would not normally be expected. Subsequent lack of contact, when this would normally be expected.

o) Inexplicable changes in ownership.

p) Activities of the trust, company or other legal entity are unclear or different from the stated purposes under trust deeds or internal regulations of the company or foundation.

q) The legal structure has been altered frequently and/or without adequate explanation (e.g. name changes, transfer of ownership, change of beneficiaries, change of trustee or protector, change of partners, change of directors or officers).

r) Management of any trustee, company or legal entity appears to be acting according to instructions of unknown or inappropriate person(s).

s) Unreasonable choice of TCSP without a clear explanation, given the size, location or specialisation of the TCSP.

t) Frequent or unexplained change of professional adviser(s) or members of management of the trustee, company or other legal entity.

u) The person giving instructions to the TCSP is reluctant to provide all the relevant information or the TCSP has reasonable grounds to suspect that the provided information is incorrect or insufficient.

v) Clients who request that transactions be completed in unusually tight or accelerated timeframes without a reasonable explanation for accelerating the transaction, which would make it difficult or impossible for TCSPs to perform a proper risk assessment.

w) Clients who insist, without adequate justification or explanation, that transactions be effected exclusively or mainly through the use of virtual assets for the purpose of preserving their anonymity.

x) Clients with previous convictions for crimes that generated proceeds, who instruct TCSPs (who in turn have knowledge of such convictions) to undertake specified activities on their behalf.

y) Clients who change their means of payment for a transaction at the last minute and without justification (or with suspect justification), or where there is a lack of information or transparency in the transaction. This risk extends to situations where last minute changes are made to enable funds to be paid in from/out to a third party.

z) The transfer of the seat of a company to another jurisdiction without any genuine economic activity in the country of destination poses a risk of creation of shell companies which might be used to obscure beneficial ownership.

aa) Clients seeking to obtain residents rights or citizenship in the country of establishment of the TCSP in exchange for capital transfers, purchase of property or government bonds, or investment in corporate entities.

Transaction/service and associated delivery channel risk - Services which may be provided by TCSPs and which (in some circumstances) risk being used to assist money launderers may include:

a) Use of pooled client accounts or safe custody of client money or assets or bearer shares, without justification.

b) Situations where advice on the setting up of legal persons or legal arrangements may be misused to obscure ownership or real economic purpose (including setting up of trusts, companies or other legal entities, or change of name/corporate seat or establishing complex group structures). This might include advising in relation to a discretionary trust that gives the trustee discretionary power to name a class of beneficiaries that does not include the real beneficiary (e.g. naming a charity as the sole discretionary beneficiary initially with a view to adding the real beneficiaries at a later stage). It might also include situations where a trust is set up for the purpose of managing shares in a company with the intention of making it more difficult to determine the beneficiaries of assets managed by the trust.

c) In case of an express trust, an unexplained (where explanation is warranted) nature of classes of beneficiaries and acting trustees of such a trust.

d) Services where TCSPs may in practice represent or assure the client's standing, reputation and credibility to third parties, without a commensurate knowledge of the client's affairs.

e) Services that are capable of concealing beneficial ownership from competent authorities.

f) Services that have deliberately provided, or depend upon, more anonymity in relation to the client's identity or regarding other participants than is normal under the circumstances and in the experience of the TCSP.

g) Use of virtual assets and other anonymous means of payment and wealth transfer within the transaction without apparent legal, tax, business, economic or other legitimate reason.

h) Transactions using unusual means of payment (e.g. precious metals or stones).

i) The postponement of a payment for an asset or service delivered immediately to a date far from the moment at which payment would normally be expected to occur, without appropriate assurances that payment will be made.

j) Successive capital or other contributions in a short period of time to the same company with no apparent legal, tax, business, economic or other legitimate reason.

k) Acquisitions of businesses in liquidation with no apparent legal, tax, business, economic or other legitimate reason.

l) Power of Representation given in unusual conditions (e.g. when it is granted irrevocably or in relation to specific assets) and the stated reasons for these conditions are unclear or illogical.

m) Transactions involving closely connected persons and for which the client and/or its financial advisors provide inconsistent or irrational explanations and are subsequently unwilling or unable to explain by reference to legal, tax, business, economic or other legitimate reason.

n) Situations where a nominee is being used (e.g. friend or family member is named as owner of property/assets where it is clear that the friend or family member is receiving instructions from the beneficial owner), with no apparent legal, tax, business, economic or other legitimate reason.

o) Commercial, private, or real property transactions or services to be carried out by the trust, company or other legal entity with no apparent legitimate business, economic, tax, family governance, or legal reasons.

p) Products/services that have inherently provided more anonymity or confidentiality without a legitimate purpose.

q) Existence of suspicion of fraudulent transactions, or transactions that are improperly accounted for. These might include:

i. Over or under invoicing of goods/services.

ii. Multiple invoicing of the same goods/services.

iii. Falsely described goods/services – over or under shipments (e.g. false entries on bills of lading).

iv. Multiple trading of goods/services.

r) Any attempt by the settlor, trustee, company or other legal entity to enter into any fraudulent transaction.

s) Any attempt by the settlor, trustee, company or other legal entity to enter into any arrangement to fraudulently evade tax in any relevant jurisdiction.

4.6 Money Services Businesses (MSB) and Money Value Transfer Services (MVTS)

4.6.1 Payment services

Risk Level: medium

Internet-based payment services provide mechanisms for customers to access, via the Internet, pre funded accounts which can be used to transfer the electronic money or value held in those accounts to other individuals or businesses. They have several characteristics that increase the TF risk, namely, non face-to-face registration, the speed and number of transactions, the limited human intervention involved in the process, and their international character. Internet-based services have been used by terrorists to store and transfer funds and to pay for the products and services needed to carry out their operations.

Case Study: PayPal accounts used for fundraising

A charity, set up in 2010, whose chairman is specialised in e-marketing, offers on its website several options to make donations by credit card, PayPal, cash transfers, checks. Over a year and a half, bank accounts of this charity received numerous donations by checks and wire transfers below EUR 500. Of the EUR 2 million collected, EUR 600 000 came from a few PayPal transactions from another country. Personal PayPal accounts were also used to collect funds, then to be withdrawn by cash, or transferred to other accounts.

Source: FATF Emerging Terrorist Financing Risks 2015

Case Study: CashU

Law enforcement identified the use of CashU accounts to anonymously engage in transactions for illicit purposes. CashU is a prepaid online and mobile payment method available in the Middle East and North Africa, a region with a large and young population with very limited access to credit cards. Because of this, CashU has become one of the most popular alternative payment options for young Arabic online gamers and e-commerce buyers. CashU was established in 2003 by Maktoob in Amman, Jordan but when Yahoo! acquired Maktoob in November 2009, the ownership of CashU was transferred to Jabbar Internet Group. Today, CashU has established offices in Dubai, Amman and Cyprus. CashU uses courier companies in the UAE to collect cash from customers. CashU is mainly used for paying for online games, VoIP, matrimonial, IT services, FX trading and download of music and software. They have a strict policy to not accept merchants providing gambling and sexual content. CashU also provides a parental control feature allowing parents to limit and control where their kids spend money online.

Source: FATF Emerging Terrorist Financing Risks 2015

Payment services are regulated and supervised by the FSC and are subject to the AML/CFT obligations contained in POCA.

Risk Indicators

- The customer opens his individual Internet account with the payment service provider in one country but logs in regularly on the website from a single or multiple third countries.
- The account opened by the customer is loaded with funds transferred from a third country, which could indicate that the customer does not live in the country from which he registered but in another country where he cannot register (not accepted by the website for security reasons) or that he registered in one country but commits illegal activities in a third country, or that he concealed the results of his illegal activities in a third country.
- The customer starts to purchase items on the Internet for amounts not in line with his previous transactions profile.
- The customer loads his Internet account with cash, if the Internet payment services provider allows loading with cash.
- The customer account with payment service provider is loaded with funds transferred by a third party apparently not related to the customer.
- The transactions of the customer suddenly deviate from its previous transactions profile after his customer account had been loaded with money from a third party.
- The customer purchases items of high value or purchases middle high value items on a regular basis with a prepaid debit card, an anonymous prepaid credit card or a gift card where the origin of the funds is difficult to retrace.
- The customer apparently resells goods purchased beforehand, without any economic reasons, or with a significant discount or increase on the price (monitoring feasible if the Internet payment service provider cooperates with the commercial website involved when analysing suspicious financial transactions);

- The buyer requests that the goods be delivered to a post office box or to a different address from the one registered to the account (facilities depending on the country of destination).
- A customer uses an account with an Internet payment service provider not to purchase items on Internet but to hide a sum of money obtained illegally. A customer opens an account with an Internet payment service provider, loads the account with important amounts of money, leaves the funds on the account during a certain period of time and requests the redemption of the funds later on.
- A customer requesting the balance from his Internet account to be transferred to a third party without apparent relation with him.
- The use of credit cards, particularly prepaid, issued in a foreign country.
- A customer sells illegal items or the goods appear on a list of forbidden items.
- Abnormality with the proposed price on an auction site or during an auction sale indicating a possible complicity between buyer and seller (a customer offers to purchase an item at a price largely higher than the requested price). Additional factors could include multiple transactions between the same buyers and sellers.
- The purchased goods are regularly shipped to a foreign country.
- The customer uses a credit card issued by a bank in an offshore centre or in a FAFT noncooperative country.
- The funds originate from a non-cooperative country.
- The country of origin of the customer is known by the FATF as a non-cooperative country in the fight against money laundering or terrorism financing.
- An unexpected turnover for a recently established commercial website or an unexpected increase in the value of the commercial website after a few sales.

4.6.2 Money value transfer services (money remitters)

Risk Level: medium

Money and value transfer services (MVTS) allow for cash to be remitted anywhere in the world without an account being required. They have proven to be particularly attractive to terrorists for funding their activities. Analysis of a number of terrorism cases has revealed that radical groups as well as persons related to terrorist organisations have used the network of registered and world-wide operating money transfer companies to send or receive money. The lack of expertise required to use the services makes it particularly attractive to terrorist groups.

The risk in Gibraltar is mitigated substantially by the fact that money remittance falls under the scope of the second payment services directive and is therefore regulated and supervised by the FSC and subject to the AML/CFT obligations contained in POCA. However, this alone does not extinguish the risk or remove the need by operators to be vigilant. Whilst there are no known cases to date, there remains the risk that a local MVTS could be used to send money to a high risk jurisdiction for onward use by a TO or that a TO uses an MVTS to send funds to Gibraltar to fund an attack or recruit FTFs either here or abroad.

Case Study: Terrorist organisation uses MVT mechanisms to move money

Person D, a leader of a terrorist organisation based in Country C and once a resident in Country A, was in hiding in Country B. The FIU in Country A found out through investigations that persons in Country A were sending money through money transfers to D's friends in Country B to financially support him. The money flow was detected because the transfers were made by nationals of Country C – which was unusual in Country A. Person D was later arrested in Country B on suspicion of terrorism. Money transfers from Country A to Country B were presented in court as supporting evidence of terrorist financing.

Source: FATF Terrorist Financing Typologies Report 2008

Case Study: Use of MVTS from Middle-Eastern countries to finance fighters to join ISIL

Ceuta and Melilla are home for many of the young Spanish recruits who were fighting in ISIL as FTFs. Although there were a wide variety of sources of revenue to pay travel costs to the conflict zones to join ISIL as a FTF, it was more difficult for young Spanish recruits in Ceuta and Melilla to purchase plane tickets due to the high long-term unemployment rate in their districts.

Analysis was conducted on 249 transfers that took place from 1 January 2014 to 31 May 2015 via three MVTS totalling EUR 117 000 sent from Syria, Iraq, Turkey and Lebanon to Ceuta and Melilla. Most of those transfers were considered suspicious because of a lack of information regarding their purpose, and no apparent relationship between senders and receivers. In addition, some of the receivers were associated with previously filed suspicious transaction reports associated with TF.

Source: FATF Emerging Terrorist Financing Risks 2015

Risk Indicators

Risk indicators for money value transfer services are confidential and therefore will be provided by GFIU directly to any operators providing these services.

4.6.3 Hawala

Hawala is a system of money transmission which arranges the transfer and receipt of funds or equivalent value. It is often reliant on ties within specific geographical regions or ethnic communities. These movements of value may be settled through trade or cash businesses engaged in remittance activities and often operate in areas of expatriate communities. Informal systems of value transfer, like Hawala, can be used for legitimate purposes, like money remittances, but also for criminal ones.

Whilst the Hawala method may be considered high risk for ML/TF purposes, Gibraltar does not have members of diaspora and migrant communities where this system would be more commonly found and local law enforcement has not found evidence to suggest that Hawala systems operate from Gibraltar, therefore, the risk posed is decreased.

4.7 Legal professionals

Risk Level: medium

Criminals and terrorist financiers seek out the involvement of legal professionals in their ML/TF activities, sometimes because a legal professional is required to complete certain transactions, and sometimes to access specialised legal and notarial skills and services which could assist the laundering of the proceeds of crime and the funding of terrorism. There is often a perception held by criminals that legal professional privilege or professional secrecy would lawfully enable a legal professional to continue to act for a client who was engaging in criminal activity or TF and/or prevent law enforcement from accessing information to enable the client to be prosecuted.

The primary risk to legal professionals of inadvertently becoming involved in TF arise from the:

- use of client accounts;
- purchase of real property;
- creation of trusts ;
- creation, merger and acquisition of companies;
- management of trusts and companies;
- setting up and managing charities;

FATF has produced a detailed report setting addressing the ML and TF vulnerabilities of legal professionals. It can be found here.

The report sets out various risk indicators, including those listed below.

Risk Indicators

The client:

1. is secretive or evasive about who they are, the reason for the transaction, or the source of funds.
2. uses an intermediary, or does not appear to be directing the transaction, or appears to be disguising the real client.
3. avoids personal contact without good reason.
4. refuses to provide information or documentation or the documentation provided is suspicious.
5. has criminal associations.
6. has an unusual level of knowledge about money laundering processes.
7. does not appear to have a business association with the other parties but appears to be connected to them.

The source of funds is unusual, such as:

1. large cash payments.
2. unexplained payments from a third party.
3. large private funding that does not fit the business or personal profile of the payer.

4. loans from non-institutional lenders.
5. Use of corporate assets to fund private expenditure of individuals.
6. Use of multiple accounts or foreign accounts.

The transaction has unusual features, such as:

1. Size, nature, frequency or manner of execution.
2. Early repayment of mortgages/loans.
3. Short repayment periods for borrowing.
4. An excessively high value is placed on assets/securities.
5. It is potentially loss making.
6. Involving unnecessarily complicated structures or steps in transaction.
7. Repetitive instructions involving common features/parties or back to back transactions with assets rapidly changing value.
8. The transaction is unusual for the client, type of business or age of the business.
9. Unexplained urgency, requests for short cuts or changes to the transaction particularly at last minute.
10. Use of a Power of Attorney in unusual circumstances.
11. No obvious commercial purpose to the transaction.
12. Instructions to retain documents or to hold money in your client account.
13. Abandoning transaction and/or requests to make payments to third parties or back to source.
14. Monies passing directly between the parties.
15. Litigation which is settled too easily or quickly and with little involvement by you.

The instructions are unusual for your business such as:

1. Outside your or your firm's area of expertise or normal business, or if client is not local to you and there is no explanation as to why a firm in your locality has been chosen.
2. Willingness of client to pay high fees.
3. Unexplained changes to legal advisers.
4. Your client appears unconcerned or lacks knowledge about the transaction.

There are geographical concerns such as:

1. Unexplained connections with and movement of monies between other jurisdictions.
2. Connections with jurisdictions which are subject to sanctions or are suspect because drug production, terrorism or corruption is prevalent, or there is a lack of money laundering regulation.

4.8 High Value and High Risk Dealers

Risk Level: low

The Office of Fair Trading licences all goods dealers in Gibraltar to carry on business. These business licences are relied upon by HM Customs as de facto import licences for the importation of the relevant goods into the jurisdiction.

The POCA imposes AML/CFT obligations on high value goods dealers (HVDs) where they sell high value goods in cash. The OFT, the AML/CFT Supervisory Authority for HVDs under the POCA, considers any dealer receiving more than £8,000 in cash for goods (in single or linked transactions) as a HVD. The OFT has issued detailed AML/CFT guidance notes for HVDs and raised awareness about HVDs' AML/CFT obligations under the POCA, which can be found using the link in 2.1.1 above. The OFT has also successfully encouraged dealers to implement cash policies not to accept cash above £8,000 for goods.

Additionally, the OFT has created a category of High Risk Dealers (HRDs) being dealers in goods which the OFT considers to have a higher inherent risk and vulnerability to ML/TF irrespective of whether sales in cash surpass the £8,000 monetary threshold.

Case Study: Terrorist use of the trade sector to move funds

An FIU received disclosures from several banks concerning account holders: Persons A and B and Company C, all active in the diamond trade. In the space of a few months, A, B and C's accounts saw a large number of fund transfers to and from foreign countries. Moreover, soon after the opening of his account, person B received several bank cheques large amounts in US dollars.

Financial information collected by the FIU showed that Company C was received large US dollar transfers, originating from companies active in the diamond industry and debited by several transfers to the Middle East in favour of Person A, a European citizen born in Africa and residing in the Middle East. One of the directors of Company C, a Belgian citizen residing in Africa, held an account at a bank in Belgium through which transfers took place to and from other countries in Europe, Africa, North America, and the Middle East. Inward transfers from foreign countries mainly took place in US dollars. These were then converted to EUR and used to make transfers to foreign countries and to accounts in Belgium belonging to Person B and his wife.

Police information collected by the FIU showed that the prosecutor had opened a file related to trafficking in diamonds originating in Africa. The largest transfers of funds by the company trading in diamonds were mainly destined to the same person, A, residing in the Middle East. Police sources revealed that both Person A and Person B were suspected of having bought diamonds from the rebel army of an African country and of smuggling them into Belgium for the benefit of a terrorist organisation.

Moreover, it appeared that certain persons and companies linked with Persons A and B had already been referred to prosecutors by the FIU in other cases for money laundering derived from organised crime.

Source: FATF Terrorist Financing Typologies Report 2008

Case Study: Terrorists use Gold to Move Value

During the invasion of Afghanistan in 2001, it was widely reported that the Taliban and members of al-Qaeda smuggled their money out of the country via Pakistan using couriers that handled bars of gold. In Karachi, couriers and hawala dealers transferred the money to the Gulf Region, where once again it was converted to gold bullion. It has been estimated that during one three-week period in late November to early December 2001, alQaeda transferred USD 10 million in cash and gold out of Afghanistan.22 An al-Qaeda manual found by British forces in Afghanistan in December 2001 included not only chapters on how to build explosives and clean weapons, but on how to smuggle gold on small boats or conceal it on the body.

Gold is often used by hawala brokers to balance their books.24 Hawala dealers also routinely have gold, rather than currency, placed around the globe. Terrorists may store their assets in gold because its value is easy to determine and remains relatively consistent over time. There is always a market for gold given its cultural significance in many areas of the world, such as Southeast Asia, South and Central Asia, the Arabian Peninsula, and North Africa.

Source: FATF Terrorist Financing Typologies Report 2008

5 Two-way communication with GFIU

5.1 Contextual information

The FATF standards require the establishment of strong operational frameworks to keep the private sector informed of emerging TF risks as they develop. Whilst the typologies, case studies and risk indicators provided in this guidance will be useful, it is important that they be supplemented with up-to-date contextual information. Such information may include real-time intelligence on an immediate threat, incidents that have been investigated and found to relate to TF, or information regarding emerging trends in Gibraltar.

GFIU will ensure that MLROs from reporting entities are provided with such information in a timely manner. This may be communicated in the form of an annual report, a periodic newsletter or more regular e-bulletins. Where necessary, GFIU may request a meeting with the MLROs from specific sectors in order to brief them on particular issues. Any case studies, typologies or risk indicators that were considered too sensitive to include in this guidance may be communicated via this channel.

5.2 Feedback on suspicious transaction reports

It is also important that reporting entities receive feedback on the suspicious transaction reports they submit. Such feedback will serve as useful guidance on their future reporting and monitoring activity and therefore enhance the detection of TF. Such feedback will be provided on the Themis platform.

6 Further Reading

The following table provides a list of relevant sources for terrorist financing, many of which have been used in the preparation of this guidance and which GFIU gratefully acknowledges.

Publications
2020 National Risk Assessment for AML/CFT and PF
FATF Financing of Recruitment for Terrorist Purposes (2018)
FATF Terrorist Financing in West and Central Africa (2016)
FATF Emerging Terrorist Financing Risks (2015)
FAFT Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (2015)
FATF Risk of Terrorist Abuse in Non-Profit Organisations (2014)
FATF Combating the abuse of non-profit organisations (2015)
FATF Virtual currencies: key definitions and potential AML/CFT risks (2014)
FATF Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals (2013)
FATF Money Laundering Using Trust and Company Service Providers (2010)
FATF Money Laundering using new payment methods (2010)
FATF Money laundering through money remittance and currency exchange providers (2010)
FATF Money Laundering and Terrorist Financing in the Securities Sector (2009)
FATF Vulnerabilities of Casinos and Gaming Sector (2009)
FATF Terrorist Financing Typologies Report (2008)
FATF Money Laundering and Terrorist Financing Through the Real Estate Sector
REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities
A Sharper Image. Advancing a Risk-Based Response to Terrorist Financing, Tom Keatinge and Florence Keen

Tom Keatinge, Florence Keen & Kayla Izenman (2019) Fundraising for Right-Wing Extremist Movements, The RUSI Journal, 164:2, 10-23, DOI: 10.1080/03071847.2019.1621479
Policy Department for Citizens' Rights and Constitutional Affairs, "Virtual currencies and terrorist financing: assessing the risks and evaluating responses" 2018

7 List of Acronyms

Acronym	Definition
AML	Anti-money laundering
CTF	Counter-terrorist financing
DLT	Distributed ledger technology
DAML	Defence Against Money Laundering
DATF	Defence Against Terrorist Financing
FAFT	Financial action task force
FTF	Foreign terrorist fighter
GFIU	Gibraltar Financial Intelligence Unit
HRD	High Risk Dealer
HVD	High value goods dealer
MLRO	Money Laundering Reporting Officer
MSB	Money Services Business
MVTS	Money and value transfer services
NPO	Non Profit Organisation
NRA	National Risk Assessment
OFT	Office of Fair Trading
POCA	Proceeds of Crime Act
STR	Suspicious Transaction Report
TCSP	Trust and Company service provider
TF	Terrorist Financing
TO	Terrorist Organisation
VA	Virtual Asset
VC	Virtual Currency

Appendix 1 – Regulated Sector

Business in the Regulated Sector.

1.(1) A business is in the regulated sector to the extent that it consists of-

(a) the acceptance by a credit institution of deposits or other repayable funds from the public, or the granting by a credit institution of credits for its own account;

(b) the carrying on of one or more of the activities listed in points 2

to 12, 14 and 15 of Annex 1 to the Capital Requirements Directive by an undertaking other than-

(i) a credit institution, or

(ii) an undertaking whose only listed activity is trading for own account in one or more of the products listed in point 7 of Annex 1 to the Capital Requirements Directive and which does not act on behalf of a customer (that is, a third party which is not a member of the same group as the undertaking);

(c) the carrying on of activities covered by the Solvency 2 Directive by an insurance company authorised in accordance with that Directive;

(d) the provision of investment services or the performance of investment activities by a person (other than a person falling within Article 2 of the Markets in Financial Instruments Directive) whose regular occupation or business is the provision to other persons of an investment service or the performance of an investment activity on a professional basis;

(e) the marketing or other offering of units or shares by a collective investment undertaking;

(f) the activities of an insurance intermediary as defined in Article 2(5) of the Insurance Mediation Directive, other than a tied insurance intermediary as mentioned in Article 2(7) of that Directive, in respect of contracts of long-term insurance within

the meaning given by Schedule 1 and 2 of the Financial Services (Insurance Companies) Act;

(g) the carrying on of any of the activities mentioned in paragraphs (b) to (f) by a branch located in a Member State of a person referred to in those paragraphs (or of an equivalent person in any other State), wherever its head office is located;

(h) the activities of the Gibraltar Savings Bank;

(i) any activity carried on for the purpose of raising money authorised to be raised under the Loan and Stock Act under the auspices of the Director of Savings;

(j) the carrying on of statutory audit work within the meaning of section 2 of the Financial Services (Auditors) Act 2009 by any firm or individual who is regulated under that Act;

(k) the activities of a person appointed to act as an insolvency practitioner within the meaning of 476 of the Insolvency Act (meaning of "act as insolvency practitioner");

(l) the provision to other persons of accountancy services by a firm or sole practitioner who by way of business provides such services to other persons;

(m) the provision of advice, aid or assistance in connection with the tax affairs of other persons by a firm or sole practitioner, whether directly or through a third party, if the firm or sole practitioner by way of business provides such advice, aid or assistance;

(n) the participation in financial or real property transactions concerning–

(i) the buying and selling of real property or business entities,

(ii) the managing of client money, securities or other assets,

(iii) the opening or management of bank, savings or securities accounts,

(iv) the organisation of contributions necessary for the creation, operation or management of companies, or

(v) the creation, operation or management of trusts, companies or similar structures,

by a firm or sole practitioner who by way of business provides legal or notarial services to other persons;

(o) the provision to other persons by way of business by a firm or sole practitioner of any of the services mentioned in subparagraph (4);

(p) the carrying on of estate agency work or letting agency work by a firm or a sole practitioner who carries on, or whose employees carry on, such work;

(q) the trading in goods (including dealing as an auctioneer) whenever a transaction involves the receipt of a payment or payments in cash of at least 15,000 euros in total, whether the transaction is executed in a single operation or in several operations which appear to be linked, by a firm or sole trader who by way of business trades in goods;

(r) the carrying on of gambling services as defined in section 7 of the Proceeds of Crime Act 2015;

(s) the auctioning by an auction platform of two-day spot or five-day futures, within the meanings given by Article 3 of the Emission Allowance Auctioning Regulation;

(t) bidding directly, on behalf of clients, in auctions of emissions allowances in accordance with the Emission Allowance Auctioning Regulation.

(u) trading, or acting as intermediary, in the sale or purchase of artistic works where the value of the transaction, or a series of linked transactions, amounts to 10,000 euros or more, by a firm or sole trader who, by way of business, trades or acts as intermediary in relation to the sale or purchase of artistic works;

(v) operating a freeport in circumstances where the operator, or any other person, by way of business stores artistic works in the freeport and the value of the artistic works so stored for a person, or a series of linked persons, amounts to 10,000 euros or more;

(w) receiving by way of business, whether on one's own account or on behalf of another person, proceeds in any form from the sale of tokenised digital assets involving the use of distributed ledger technology or a similar means of recording a digital representation of an asset;

(x) the carrying on by a firm or sole practitioner by way of business, in or from Gibraltar, of activities relating to the use of distributed ledger technology for storing or transmitting value belonging to others for the purposes of paragraph 10 of Schedule 3 of the Financial Services (Investment and Fiduciary Services) Act, as amended extended or re-enacted.

(2) For the purposes of subparagraph (1)(a) and (b) "credit institution" means–

(a) a credit institution as defined in Article 4(1)(1) of the Capital Requirements Regulation; or

(b) a branch (within the meaning of Article 4(1)(17) of that Regulation) located in an member state of an institution falling within paragraph (a) (or of an equivalent institution in any other State) wherever its head office is located.

(3) For the purposes of subparagraph (1)(n) a person participates in a transaction by assisting in the planning or execution of the transaction or otherwise acting for or on behalf of a client in the transaction.

(4) The services referred to in subparagraph (1)(o) are

(a) forming companies or other legal persons;

(b) acting, or arranging for another person to act-

(i) as a director or secretary of a company,

(ii) as a partner of a partnership, or

(iii) in a similar position in relation to other legal persons;

(c) providing a registered office, business address, correspondence or administrative address or other related services for a company, partnership or any other legal person or arrangement;

(d) acting, or arranging for another person to act, as-

(i) a trustee of an express trust or similar legal arrangement; or

(ii) a nominee shareholder for a person other than a company whose securities are listed on a regulated market.

(4A) For the purposes of sub-paragraph (1)(p), "letting agency work" shall have the meaning given to it in section 7 of the Proceeds of Crime Act 2015. (4B) For the purposes of sub-paragraph (1)(u), "artistic work" shall have the meaning given to it in section 7 of the Proceeds of Crime Act 2015.

(4C) For the purposes of sub-paragraph (1)(v), "freeport" shall have the meaning given to it in section 7 of the Proceeds of Crime Act 2015.

(5) For the purposes of subparagraph (4)(d) "regulated market"–

(a) in relation to any Member State, has the meaning given by point 14 of Article 4(1) of the Markets in Financial Instruments Directive; and

(b) in relation to any other State, means a regulated financial market which subjects companies whose securities are admitted to trading to disclosure obligations which are contained in international standards and are equivalent to the specified disclosure obligations.

(6) For the purposes of subparagraph (5) "the specified disclosure obligations" means–

(a) disclosure requirements set out in Articles 17 and 19 of Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (market abuse regulation);

(b) disclosure requirements consistent with Articles 3, 5, 7, 8, 10, 14 and 16 of Directive 2003/71/EC of the European Parliament and of the Council of 4 November 2003 on the prospectuses to be published when securities are offered to the public or admitted to trading;

(c) disclosure requirements consistent with Articles 4 to 6, 14, 16 to 19 and 30 of Directive 2004/109/EC of the European Parliament and of the Council of 15 December 2004 relating to the harmonisation of transparency requirements in relation to information about issuers whose securities are admitted to trading on a regulated market; or

(d) disclosure requirements consistent with EU legislation made under the provisions mentioned in paragraphs (a) to (c).

(7) For the purposes of subparagraph (1)(j) and (l) to (q) "firm" means any entity, whether or not a legal person, that is not an individual and includes a body corporate and a partnership or other unincorporated association.

(8) For the purposes of subparagraph (1)(q) "cash" means notes, coins or travellers' cheques in any currency.

(9) For the purposes of subparagraph (1)(s) "auction platform" means a platform on which auctions of emissions allowances are held in accordance with the Emission Allowance Auctioning Regulation.

Excluded Activities.

2.(1) A business is not in the regulated sector to the extent that it consists of-

(a) the issuing of withdrawable share capital within the limit set by section 28 Co-operative Societies Act (maximum interest in a society's withdrawable shares), or the acceptance of deposits from the public within the limit set by rule 20 of the Cooperative Society Rules (carrying on of banking by societies), by a society registered under that Act; or

(b) the engaging in financial activity which fulfils all of the conditions set out in paragraphs (a) to (g) of subparagraph (3) of this paragraph by a person whose main activity is that of a high value dealer;

(c) a business named in an Order made by the Minister for such purposes.

(2) For the purposes of subparagraph (1)(e) a "high value dealer" means a person mentioned in paragraph 1(1)(q) when carrying on the activities mentioned in that paragraph.

(3) A business is not in the regulated sector to the extent that it consists of financial activity if–

(a) the person's total annual turnover in respect of the financial activity does not exceed £64,000;

(b) the financial activity is limited in relation to any customer to no more than one transaction exceeding 1,000 euros, whether the transaction is carried out in a single operation, or a series of operations which appear to be linked;

(c) the financial activity does not exceed 5% of the person's total annual turnover;

(d) the financial activity is ancillary to the person's main activity and directly related to that activity;

(e) the financial activity is not the transmission or remittance of money (or any representation of monetary value) by any means;

(f) the main activity of the person carrying on the financial activity is not an activity mentioned in paragraph 1(1)(a) to (p) or (r); and

(g) the financial activity is provided only to customers of the person's main activity and is not offered to the public.

(4) A business is not in the regulated sector if it is carried on by(a) the Financial Secretary of the Government of Gibraltar; or

(b) the Registrar of the Supreme Court, when acting as trustee in his official capacity.

Interpretation.

3.(1) In this Part-

"the Capital Requirements Regulation" means Regulation (EU) No 575/2013 of the European Parliament and of the Council, as the same may be amended from time to time;

"the Emission Allowance Auctioning Regulation" means Commission Regulation (EU) No 1031/2010 of 12 November 2010 on the timing, administration and other aspects of auctioning of greenhouse gas emission allowances pursuant to Directive 2003/87/EC of the European Parliament and of the Council establishing a scheme for greenhouse gas emission allowances trading within the Community, as the same may be amended from time to time;

"the Insurance Mediation Directive" means directive 2002/92/EC of the European Parliament and of the Council of 9th December 2002 on insurance mediation, as the same may be amended from time to time; and

"the Markets in Financial Instruments Directive" means directive 2004/39/EC of the European Parliament and of the Council of 12th April 2004 on markets in financial instruments, as the same may be amended from time to time;

"the Solvency 2 Directive" means Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II), as the same may be amended from time to time.

(2) In this Part references to amounts in euros include references to equivalent amounts in another currency.

(3) Terms used in this Part and in the Capital Requirements Regulation or the Markets in Financial Instruments Directive have the same meaning in this Part as in those Directives.