Appendix L

Terrorist Financing Typologies and Countering the Financing of Terrorism Guidance

Introduction

The purpose of this document is to provide specific guidance for all businesses in the regulated sector which may be vulnerable to misuse by those who wish to finance terrorism. The document will provide some detail of the ways in which terrorist financing takes place building from the brief definition of the term found at 7.3.2 of the main body of the Handbook. A number of typologies are set out along with a description of countermeasures which businesses in the regulated sector should adopt. This guidance should be read in conjunction with the main body of the Handbook. As with all guidance in the Handbook, this guidance is not law, however it is persuasive. Where a person follows guidance this would tend to indicate compliance with the legislative provisions and vice versa.

What is Terrorist Financing?

Section 7.3.2 of the main body of the Handbook provides a general definition as to what constitutes terrorist financing. The term is a generic one which is not defined in any Isle of Man Statute, but was set out in the United Nations International Convention for the Suppression of the Financing of Terrorism (Terrorist Financing Convention) 1999 and includes the financing of terrorist acts, terrorist organisations or individual terrorists. The various terrorist financing offences can be found in Part III of the Anti-Terrorism and Crime Act 2003. These include the offences of:

- Fund raising (section 7);
- Use and possession (section 8);
- Facilitating funding (section 9);
- Financing travel (section 9A);
- Money laundering (section 10); and
- The Failure to Disclose: regulated sector offence (section 14).

It is particularly important to note that whilst the *mens rea*[1] for the other offences require knowledge or reasonable cause to suspect use for terrorist purposes, the offence of Facilitating funding can also be committed when the *offender has failed to exercise due diligence as to whether it will or may be used for the purposes of terrorism*.

The direct (estimated) costs involved in carrying out terror attacks have been quite widely reported. The table below gives an indication of the approximate costs of some of the more recent high profile attacks.

Date	Attack	Country	Estimated Cost
12 October 2000	USS Cole bombing	Aden (Yemen)	USD 10,000

[1] 'guilty mind', having awareness that the act is criminal

12 October 2002	Bali bombings	Bali	USD 50,000
11 March 2004	Madrid train bombings	Spain	USD 10,000
7 July 2005	London transport bombings	UK	GDP 8,000
13 November 2015	Paris attacks	France	EUR 27,000
14 July 2016	Nice truck attack	France	EUR 2,500
22 May 2017	Manchester Arena bombing	UK	Investigation ongoing
3 June 2017	London Bridge attack	UK	Investigation ongoing

As can be seen the direct cost of each of these attacks is relatively low and appears to be decreasing, particularly with the recent use of unsophisticated, inexpensive but effective *modus operendi*.

Because of the high profile given to the direct costs, it is easy to obscure the bigger picture. The broader operational costs which underpin terrorist activity are significantly higher and include:

- The costs involved in promoting a militant ideology;
- Paying operatives and often their families expenses such as subsistence;
- Death in service – when terrorists die, the terrorist organisation often supports the family;
- Arranging for travel for training and to stage attacks;
- Training new members;
- Buying or renting safe houses;
- Forging documents;
- Paying bribes; and
- Acquiring weapons.

Many of these expenses will, by necessity, be incurred in secret and will therefore incur a “clandestine premium”. In addition, the source of the funds used must be obscured to prevent that source being disrupted. As these operational costs are quite high, terrorist organisations are dependent on a steady, sustained funding stream.

Terrorist Financing Typologies

The following information and typologies have largely been extracted from a recent Financial Action Task Force (“FATF”) report entitled *Emerging Terrorist Financing Risks* dated October 2015 (link below).

http://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf

The need for terrorist groups to obtain funds, move and use them has always been there, but as terrorist groups have evolved, so too have the methods they use in order to do this. The FATF refer to these recent developments as “emerging TF risks”. Although there is much overlap between the methods used by large terrorist

organisations, small terrorist cells, lone actors and foreign terrorist fighters ("FTFs"), some distinctly different patterns can be seen which will be outlined below. For more detail on these, please refer to the FATF paper above.

Traditional Terrorist Financing

Fund raising

The mainstream methods used by terrorist organisations to raise funds include the following:

- Private donations by terrorist sympathisers;
- Abuse and misuse of Non-Profit Organisations ("NPOs");
- Criminal activity; and
- Legitimate commercial activity.

Of these, probably the second and fourth may have most relevance to businesses in the regulated sector in the Isle of Man.

Abuse and misuse of NPOs

This is one of the most important methods by which mainstream terrorist organisations use to raise funds. A 2014 FATF study found that the abuse or misuse of NPOs occurred in five different ways:

- Diversion by embedded terrorist sympathisers of donations made to legitimate NPOs to terrorist organisations;
- Exploitation of legitimate NPOs;
- Misuse of the NPO delivery programme to support the terrorist organisation; and
- Creation of sham NPOs.

The study found that NPOs at most risk of terrorist abuse are those engaged in activities which are operating close to an area where terrorist activity is taking place. NPOs that remit funds to counterpart or correspondent NPOs located in such areas are vulnerable to misuse unless effective due diligence is done on the counterpart NPO with proper auditing of how and where the funds are used. The study found that NPOs operating in such areas are at an increased risk of being infiltrated and exploited by terrorist groups, particularly where less-established or start-up charities or NPOs without effective due diligence procedures are involved.

Legitimate commercial activity

A number of law enforcement investigations have found links between genuine commercial enterprises and terrorist organisations where the profits of the business were used to provide finance for the terrorist cause. Examples have included the shipment of used cars to West Africa and to the Middle East with some of the revenue from the sale of those cars being used to support terrorist groups. Corporate services providers who may unwittingly be involved in such commercial activity and banks should be aware of such typologies.

Movement of funds

Any method which can be used to transfer funds is potentially vulnerable to misuse for terrorist financing including the following:

- Fund transfers through banks;
- Money transmission services;
- Physical transportation of cash

Banking

The banking sector remains vulnerable to misuse for terrorist financing as it remains the most efficient and reliable way to transfer funds internationally and several FATF reports have commented on the use of the bank accounts of NPOs to move funds to terrorist organisations. It is attractive to terrorist groups because of the speed and ease by which it can be used to transfer funds within the global financial system. The global banking system is so large that terrorist fund movements have the opportunity to blend in with normal financial activity and avoid attracting attention. Terrorist fund movements may often be relatively small in comparison with legitimate commercial fund movements and therefore not arouse suspicion. Studies have found typologies including the deposit of cash in a personal bank account followed by international fund transfers, the use of legitimate and shell business accounts and the use of debit cards by terrorist groups to withdraw funds from accounts opened by terrorist sympathisers.

Money transmission services

This sector is also vulnerable to misuse for terrorist financing, particularly in those regions where access to banking services is limited. As migrant communities and families rely heavily on money transmission services to send funds home, this provides an opportunity to mingle terrorist financing fund movements with legitimate family transfers making them difficult to detect. Studies have also reported the use of money transmission services to finance foreign terrorist fighters.

Physical transportation of cash

Cash remains the medium most used by terrorist organisations. Funds may be raised in many ways and transferred globally using the international banking system or money transmitters, but they are often converted into cash before being taken into conflict zones and used.

Emerging Terrorist Financing Risks

Foreign terrorist fighters (“FTFs”)

In September 2014 the United Nations Security Council defined foreign terrorist fighters as individuals who travel or attempt to travel to a state other than their state of residence or nationality “for the purpose of the perpetration, planning or preparation of or participation in terrorist acts or the providing or receiving of terrorist training”.

FTFs are not new, but the conflict in Syria and Iraq has led to a significant escalation in their involvement in terrorist activity. An estimated 30,000 FTFs currently operate in this region. Returning FTFs also represent a new and dangerous threat of terrorist activity in their country of origin. Self-funding by individuals and funding by recruitment and facilitation networks are considered to be the main methods used to raise funds for FTFs.

The funding levels required by FTFs are relatively low and are required to support transportation, accommodation whilst en-route to areas of conflict, outdoor clothing, camping equipment, mobile phones, food and general living expenses.

FTFs often use funds from legitimate sources such as employment income, family support, social assistance, student grants and the sale of personal belongings and assets purchased on credit just before their planned travel. Other typologies include the FTF taking out small short-term loans, often from multiple lenders that they have no intention of ever repaying.

FTFs fund movements usually involve the physical transportation of cash, the use of ATMs to access funds held in bank accounts and money transmission services.

Other methods of raising and moving funds

Newer emerging methods include:

- Fundraising using social media; and
- Crowd funding

To raise funds and

- Virtual currencies;
- Prepaid cards; and
- Internet-based payment services

To transfer and/or access funds.

Countering the Financing of Terrorism Guidance

The key to countering the financing of terrorism is firstly to be aware that it can happen and that it can involve any jurisdiction including the Isle of Man. The above typologies give an indication of the various methods which can be used to raise and remit funds and all businesses in the regulated sector should be aware of them.

Effective implementation of the provisions of the Anti-Money Laundering and Countering the Financing of Terrorism Code 2015 (“the Code”) is critical so that activity which leads to a suspicion of terrorist financing is identified and an SAR made promptly to the FIU.

No businesses in the regulated sector are immune from being used for terrorist financing, but the following sectors may be particularly vulnerable:

- Banking sector;

- Money transmission Services;
- Non-profit organisations:
- Corporate service providers.

It is essential that businesses apply effective customer due diligence, not only to determine who their customers are; but also, probably of more importance, to determine the nature and intended purpose of the business relationship. If that business relationship is likely to involve remittance of funds to or business activity in other jurisdictions, further enquiries should be pursued at the onset of the relationship as to the nature, level, frequency and purpose of such remittances or business activity. These enquiries will also form part of the customer risk assessment and if remittances or activity are likely to involve jurisdictions which bear a higher risk of terrorist financing, areas of conflict or neighbouring regions, consideration should be given to raising the risk rating of the customer to higher risk and obtaining enhanced due diligence as per paragraph 15 of the Code. The customer risk assessment and customer due diligence should give the relevant person a baseline view of what is likely to be normal and effective ongoing monitoring should identify unusual or suspicious activity. Remittance of funds to or business activity in higher risk jurisdictions may lead the relevant person to perform further scrutiny and institute further enquiries as to the nature and purpose of those remittances or activity.

Proper screening of the screening of both the customer and any proposed or actual recipient of funds or business services may be appropriate in the circumstances detailed above.

Unusual activity may include, but is not limited to:

- Unusual customer behaviour;
- Cash transfers to higher risk places or transit countries (e.g. Turkey) either through the bank or through Money transmitters;
- Lots of cash transactions;
- Customers who may have banked for a long time, even have a dormant account which has been suddenly reactivated;
- Lots of money for transport expenditure to higher risk locations;
- Consumer loans which are not then repaid;
- Contributions to relevant charities;
- On social media, lots of “new friends” especially over a wide geographical area;
- Funds in from crowd funding or donation sites.