Republic of Namibia

Financial Intelligence Centre

FINANCIAL INTELLIGENCE CENTRE (FIC)

REPUBLIC OF NAMIBIA

P.O.BOX 2882, Windhoek

Tel: + 264 61 2835100, Fax +264 61 2835259

Web address: www.fic.na

E-mail address: helpdesk@fic.na

CIRCULAR NO. 35 OF 2015

ON

AWARENESS CREATION ON EMERGING TERRORIST FINANCING RISKS

DECEMBER 2015

1. Introduction

The Financial Intelligence Centre's (FIC)'s primary objective is to assist the Government of the Republic of Namibia to reduce the National Money Laundering (ML), Terrorist Financing (TF) and Proliferation Financing (PF) risks to tolerable levels. In October 2015, the Financial Action Task Force (FATF) issued a report titled: *Emerging Terrorist Financing risks*. The FIC is issuing this circular which summarizes key findings of the said report. The report is attached to this circular. The primary objective of this circular is to create awareness on emerging TF risks amongst relevant stakeholders including regulatory and supervisory bodies, law enforcement authorities, accountable and reporting institutions etc. The emerging trends are presented as findings for relevant stakeholders to note the specific trends and methods used by terrorists and terrorist organizations.

It should be further noted that effective implementation of the FATF Recommendations the Financial Intelligence Act, 2012 (Act No 13 of 2012)(FIA) and the Prevention and Combating of Terrorist and Proliferation Activities Act, 2014 (Act No. 4 of 2014)(PACOTPAA) provide the necessary AML/CFT framework to address the TF risks identified in the report. This circular will therefore not be discussing the known obligations of various stakeholders in mitigating TF risks, as contained in both the FATF Recommendations, the PACOTPAA and the FIA.

2. Background

It has been noted that while the number and type of terrorist groups and related threats have changed over time, the basic need for terrorists to raise, move and use funds has remained the same. However, as the size, scope and structure of terrorist organisations have evolved, so too have their methods to raise and manage funds. The main objective of the FATF report on emerging TF risks is to analyse recently identified TF methods and phenomena, referred to as 'emerging TF risks'.

The report further aims to analyse recently identified TF methods and phenomena, referred to as emerging TF risks. The report will also provide an overview of

traditional methods, techniques and tools in which funds are raised, moved and stored by terrorists and terrorist organisations to assess their current significance.

Importantly, the report also highlights that understanding how a terrorist organisation manages its assets is critical to starving the organisation of funds and disrupting their activities in the long term. Terrorist organisations have different needs, depending on whether they are large, small, or simply constituted of a network of seemingly isolated individuals. The section on financial management in the report explores the use of funds by terrorist organisations, not only for operational needs but also for propaganda, recruitment and training, and the techniques used to manage these funds, including allocating specialised financial roles. The report also finds that authorities need to do further work to identify and target various entities responsible for these functions.

This circular aims to create awareness of emerging TF risks, including the threats and vulnerabilities posed by:

- foreign terrorist fighters (FTFs);
- fundraising through social media;
- new payment products and services, and
- the exploitation of natural resources.

3. Summary of emerging TF risks

3.1 Foreign Terrorist Fighters (FTFs)

The FTF phenomenon is not new, but the recent scaling up of individuals travelling to Iraq and Syria has been a challenge for many FATF members. FTFs are predominantly using traditional methods, particularly self-funding, to raise the funds they require to travel to the conflict areas. However, the novel aspect for jurisdictions is the challenge in identifying these individuals because of the relatively low amounts of funding they require and the speed with which they can acquire it. The report reveals that financial intelligence can assist in identifying FTFs in a number of ways. Close cooperation between authorities domestically and internationally and close

partnerships between authorities and the private sector can assist to better identify FTFs and their facilitation networks. The report also shows that further work is required to shed light on blind spots in information about FTFs, including returnees.

Listings of individuals and entities on the ISIL (Da'esh) & Al-Qaida Sanctions List is a powerful and effective instrument to implement sanctions provisions and therefore hinder ISIL or ANF's ability to generate revenue through the illicit trade in various goods such as crude oil, antiquities etc. It is essential that Accountable and Reporting Institutions prudently and effectively screen their client base against updated versions of the ISIL (Da'esh) & Al-Qaida Sanctions List. If matches are noted in such screening, such matches must be reported to the FIC timely.

3.2 Fundraising through social media

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

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

The use of organised crowdfunding techniques also represents an emerging TF risk. Crowdfunding is an Internet-enabled way for businesses, organisations, or individuals to raise money, from donations or investments, from multiple individuals. Crowdfunding websites allow people to easily set up a fundraising page and collect donations. Yet, crowdfunding is vulnerable to exploitation for illicit purposes, including instances where the true purpose of the funding campaign is masked. Individuals and organisations seeking to fundraise for terrorism and extremism support may claim to be engaging in legitimate charitable or humanitarian activities and may establish NPOs for these purposes. Several cases indicate that the end-use of funds collected through crowdfunding and social networks was not known to donors.

3.2.1 Challenges associated with the use of social media

There are a number of interrelated countering the financing of terrorism (CFT) systems challenges associated with the use of the social media to raise funds. Some are as follows:

- Often, it is not possible to distinguish between the sympathisers, supporters and actual terrorists;
- Due to false declaration of fundraising purposes, the identification of persons contributing money, either intentionally or unwittingly, is a serious challenge to competent authorities;
- It is often difficult to get evidence of the use of funds when transferred via the Internet;
- Social networks are used to show the relationships, but finding proof of TF is still difficult.

The report also states that countries make considerations on possibilities to monitor, block or remove websites to prevent their use (where law applies and while keeping in mind and respecting privacy and human rights). Further discussions could be considered about the possibilities of referring crowdfunding platforms and other companies as reporting entities and adapting legislation and regulations on new payment methods.

From an AML regulatory and supervisory body's point of view, more work remains to be done to better leverage social media information for investigative purposes and including it as court evidence. Competent authorities could share additional strategic information with reporting entities via clear legal channels. In that regard, the competent authorities should consider further collaboration with the private sector to get access to more data and analysis, including adapting fields in reporting requirements for online information.

3.3 New payment products and services

This report finds that electronic, on-line and new payment methods pose an emerging TF vulnerability which may increase over the short term as the overall use and popularity of these systems grows. Many of these systems can be accessed globally and used to transfer funds quickly. While transactions may be traceable, it proves difficult to identify the actual end-user or beneficiary. This report presents a number of interesting cases, but the actual prevalence and level of exploitation of these technologies by terrorist groups and their supporters is not clear at this time and remains an ongoing information gap to be explored, in combatting TF.

3.3.1 Challenges associated with new payment products and services

The rapid development, increased functionality, and growing use of new payment products and services (NPPS) globally have created AML challenges for countries and private sector. Notwithstanding the known vulnerabilities, the actual prevalence and level of exploitation of these technologies by terrorist groups and their supporters is not clear at this time and remains an ongoing information gap to be explored.

3.4 The exploitation of natural resources

The exploitation of natural resources for TF was raised as a substantial concern in the context of the Islamic State of Iraq and the Levant (ISIL) but this report has confirmed that it is also relevant for other terrorist organisations and regions. The ability to reap high rewards from the natural resources sector – coupled with the weak institutional capability, particular in or near areas of conflict, creates a significant vulnerability for terrorist organisations to capitalise on. The report finds that this issue is linked with criminal activity including extortion, smuggling, theft, illegal mining, kidnapping for ransom, corruption and other environmental crimes.

3.4.1 Challenges associated with exploitation of natural resources

The investigation of crimes associated with the natural resources sector, including TF-related investigations, are often complex and requires extensive financial analysis. It is often difficult to identify the entire criminal network and specific actors (including facilitators) who are committing these crimes. This also leads to challenges in the prosecution of these crimes. It is important to identify all the operators in the sector, both legal and illegal, in order to take steps to deal with the illegal operators through law enforcement measures. Additionally, targeting smugglers and smuggling networks, which often extend beyond the source country of the natural resources in addition to the area in the immediate control of the group, will assist in combating this method of raising funds.

In order to overcome these challenges it will be necessary to consider how the public and private sectors can collaborate and include actors outside of the traditional scope of the AML/CFT regime. Strengthening legislative and regulatory frameworks within these sectors is also critical. This is especially true given the vast sums that terrorist groups can generate through the exploitation of natural resources. To adequately tackle these issues, the public and private sectors need to be aware of the vulnerabilities of this sector as the possible links of TF to corruption and organised crime.

4. Conclusion

While terrorist organisations are continuing to adapt and counter law enforcement responses, it is clear that they continue to require resources to meet their destructive goals. Following the financial trail, and understanding how all types of terrorist organisations, whether large territorially-based or small cells operating autonomously, need, use and manage funds is critical in detecting, preventing and sanctioning terrorist and terrorist financing activity. Understanding and exchanging information on the financial management of terrorist organisations is important in order to implement CFT measures effectively.

Financial intelligence is a necessary component for all counter terrorism activities, and use of relevant and appropriate non-financial information is essential for TF investigations.

In conclusion, this report is intended to assist relevant AML regulators, supervisory bodies, law enforcement authorities and the private sector to implement robust CFT systems which take into account changing TF risks, trends and methods. As stated in the introductory paragraph, the FATF Recommendations and The FIA provide the necessary AML/CFT framework to address the TF risks identified in the report but effective implementation of these standards is key. For instance, developing national, or specific, terrorist financing risk assessments will provide a basis for implementing a risk-based response to addressing TF. The use of these risk assessments to conduct strategic analysis of current TF risks will help inform policy makers implement the necessary legal and operational measures.

5. Non-compliance with the provisions of this Circular

This circular is issued in terms of Section 9(1) (h) of The FIA. Although the circular is issued to enhance awareness on emerging TF, the relevant risk mitigation provisions are contained in the PACOTPAA and the FIA and the complementing Regulations and Guidance Notes. Any non-compliance, were such is expected to mitigate relevant risks as contained in this circular is an offence in terms of section 63 of The FIA.

The information contained in this document is intended only to provide a summary and a general overview on these matters and is not intended to be comprehensive. This document may contain statements of policy which reflect FIC's administration of the legislation in carrying out its statutory functions.

The guidance provided by the Centre in this circular, even though authoritative, is not intended to replace the FIA or PACOTPAA including Regulations issued thereunder.

The information contained herein is current as at the date of this document.

Date issued: 22 December 2015

Director: Financial Intelligence Centre