21 ISSUE

Financial Intelligence Office Newsletter

Inside this issue

Suspicious Transaction Reports Statistics (2018)

Number of STRs	2018	2017
From Financial Institutions and Insurance Companies	1,122 (30.2%)	746 (24.2%)
From Games of Fortune Operators	2,087 (56.2%)	2,074 (67.2%)
From Other Institutions	507 (13.6%)	265 (8.6%)
Total	3,716	3,085

- **The total number of STRs received by *GIF* from 2018 has increased by 20.5%, as compared with the same period in 2017.**
- **STRs received from financial sector and gaming sector constituted 30.2% and 56.2% of total respectively.**
- **A total of 121 STRs were sent to the Public Prosecutions Office from 2018.**

International Trend—Non-Profit Organization

Introduction

According to the Anti-Money Laundering and Counter-Terrorist Financing (AML/CFT) standard setting body "Financial Action Task Force (FATF)", the interpretive note to Recommendation 8 indicated that Non-Profit Organizations (NPOs) may be exploited for terrorist financing purposes for a variety of reasons. NPOs enjoy the public trust, they have the opportunity to access to considerable sources of funds, and are often cash-intensive. In addition, some NPOs have branches around the world that provide a framework for the NPOs to conduct charitable activities and financial transactions locally and overseas. However, many of these branches are located in or close to areas where terrorist activities are prevalent. Therefore, terrorist organizations can infiltrate NPOs and misuse charitable funds and charitable work to cover for, or support terrorist activities.

To prevent NPOs from being exploited for terrorist financing purposes, and not to hinder charitable and humane work for legitimate purposes, FATF revised its recommendation for NPOs in 2016, all jurisdictions should use a risk-based approach and apply focused and proportionate measures for NPOs to prevent them from terrorist financing abuse. The main purpose of the amendments was to avoid over regulation and disruption of charitable activities, and to avoid losing resources or assistances to those in need. Extensive saying and inference that all NPOs are high risk is inappropriate and disproportionate.

(Reference : FATF Recommendation 8 - Interpretative Note)

International Trend—Non-Profit Organization

FATF Definition of NPO

NPO is a legal person or arrangement or organization that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of "good works".

Risk of NPO defined by international organization

Risk can be defined as the potential harm as a result of a threat exploiting a vulnerability (Threat + Vulnerability = Risk). The threats facing NPOs in the context of terrorist abuse are individuals or groups who support terrorist organization, while the vulnerabilities are a legitimate NPO be exploited by internal or external individuals, who put the organization at risk; or an individual may create an illegitimate NPO, which put the NPO sector's legitimacy and reputation at risk.

NPOs with higher risk of terrorist financing abuse appear to be those that:

* Are engaged in service activities, including housing, social services, education and health care;
* Operate in close proximity to an active terrorist threat, which refers to an NPO operating in an area of conflict where there is an active terrorist threat, or to an NPO that operates locally, but within a population that is actively targeted by a terrorist movement for support and cover.

Some examples of risk indicators of NPOs are as follows:

* Financial reports are not clear and confusing;
* NPO funds are transferred to entities not associated with declared activities;
* NPO transactions are structured to avoid transaction reporting
* No documentation on use of funds;
* Little or no history of legitimate charitable activities;
* Media reports the NPO is linked to known terrorist organizations or entities that are engaged, or suspected to be involved, in terrorist activities;
* Parties to the transactions (e.g. account owner, sender, beneficiary or recipient) are from known jurisdiction to support terrorist activities and organizations;
* NPO raises funds from a major public event and then authorizes a third party to be a signatory to the NPO account, who uses it to send funds to high-risk jurisdiction;
* Unusual or atypical large cash withdrawals, particularly after the financial institution refuses to wire NPO funds overseas (thus raising cross-border cash smuggling suspicions);
* Vague justifications and a lack of documentation when the financial institution questions NPO requests to transfer funds to high-risk locations or entities;
* NPO account shows signs unexplained increases in deposits and transaction activity.

(Reference : FATF report "Risk of Terrorist Abuse in Non-Profit Organisations" published in June 2014 & "Non-profit Organizations & Terrorism Financing Red Flag Indicators 2018" launched at CTF Summit 2018)

Overview of NPOs in Macao

Despite the large number of NPOs registered in Macao, only a relatively small number of NPOs actually meet FATF's definition of NPOs with risk on terrorist financing abuse. The majority of NPOs in Macao are set up by local associations for specific purposes such as sport, charity and culture. Most of the active associations in Macao are funded by the Macao SAR government. Therefore, the form and purpose of NPOs' activities are subject to government's supervision. According to previous analysis, the proportion of cross-border transactions of NPOs in Macao was not high, only a small number of sources and destinations of funds may involve in regions with high risk of terrorist financing.

In accordance with the requirements of the FATF, Macao is required to conduct regular risk assessments of NPO continuously. GIF has been paying attention to the risk assessment of NPO. At the same time, different educational or promotional programs will be performed to raise the awareness of the risks involved in NPOs, so as to prevent terrorist financing risks.

Case Study

Case 1: Suspicious Non-Profit Organization activity related to terrorist financing

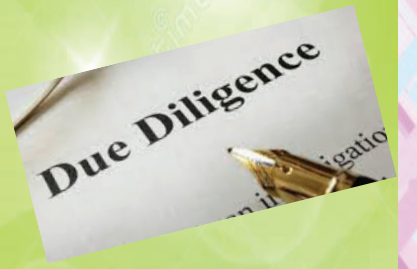
An NPO received electronic funds transfers from multiple third parties, and frequent large cash deposits into its NPO bank account. The NPO had links to a religious organisation that was associated with violent extremist views according to the media's report. Some entities transferring funds into the NPO account were reportedly linked to terrorist groups or entities. While the majority of the funds were traced as going to local charitable activity, some of the funds remained unaccounted for and it raised suspicions about their ultimate use.

(Reference : "Non-profit Organizations & Terrorism Financing Red Flag Indicators 2018" launched at CTF Summit 2018)

Red Flags:

* Media reported that the NPO was linked to known terrorist organisations or entities that were engaged, or suspected to be involved, in terrorist activities;
* Related parties of the transaction (for example: account owner, sender, beneficiary or recipient) were from jurisdictions known to support terrorist activities and organisations;
* NPO's account showed signs of unexplained increases in deposits and transaction activity, without apparent association to its charitable activities.

Recommendations:



* Pay more attention to news/media reports and the latest international trends of ML/TF so as to assist in detecting any suspicious transactions in relation to NPOs;
* Conduct enhanced customer due diligence for frequent large cash deposits transactions made by NPOs;
* Pay attention to the details of the account holders/signatories and be alert to any possible associated accounts held within the financial institution, with signs of linkage to terrorist financing.

Case 2 Suspected involvement in online romance scam

A local resident Miss A claimed to be a clerk. Miss A went to Bank K to open a bank account and then received multiple cash deposits through ATM, with similar amount for each deposit. After receiving the funds, she remitted similar funds to a company account in Country X. Miss A claimed that she knew Mr. B from internet social media and claimed that a gift was mailed to her from Mr. B but was detained by relevant authorities in Country X. Since the gift contained jewelleries, Miss A claimed that she had to remit the funds to the company in Country X in order to pay customs duties on her behalf to redeem those jewelleries. During this period, Miss A had insufficient account balance, so she had to deposit cash via ATM and claimed that source of funds was borrowed from her friends. Bank K suspected that Miss A was being deceived so Bank K reported the case to FIU.

After further investigation by FIU, Miss A was found to be a VIP client with lots of deposits in Bank L, therefore she could enjoy discount on bank fees and foreign currency exchange rates in Bank L. However, Miss A chose to open a new account in Bank K with ATM cash deposits from different third parties without any discount on bank fees. Her behavior is contrary to the normal cost and benefit principle. It is even more suspicious that the funds were remitted to an overseas company, rather than to the local government department or to Mr. B himself. In addition, intelligence revealed that Miss A and Mr. B were involved in an overseas online romance scam and were being investigated by local law enforcement agencies. After analysis, the case had the characteristics of online romance scam. Although Miss A seems to be a victim of online romance scam, she actually assisted the criminals to collect illicit funds and then transferred the funds overseas.

Red Flags:

- It is possible for a criminal to disguise as a victim in order to reduce the wariness of financial institutions to identify suspicious transactions;
- Cash transactions through ATM to conceal the actual sources of fund;
- Cash is deposited into the account just before the remittance transaction, the amount of each cash deposit is similar, and the source of cash is in doubt;
- Failure to provide the bank with reasonable explanations of transaction, the relationship between the sender and the beneficiary of the remittance is doubtful.

Recommendations:

- Ensuring that the system can detect trends in suspicious transaction typologies that change from time to time;
- Pay special attention to the background of counterparties in suspicious transactions as well as complying the obligations of performing adequate customer due diligence;
- If suspicious transaction is detected, reporting entity should request the client for supporting documents and reasons of transactions. If explanation cannot justify such transactions, reporting entity should submit suspicious transaction report to FIU.

contact us

Published in May 2019
Published by:
Financial Intelligence Office,
Macao SAR Government

Address:
Avenida Dr. Mário Soares, Nos. 307-323, Edifício "Banco da China", 22ºandar, Macau

Tel:
(853) 2852 3666
Fax:
(853) 2852 3777

E-mail:
info@gif.gov.mo
Website:
http://www.gif.gov.mo

If you have any suggestions and enquiries on this newsletter, or like to have more copies, please feel free to contact *GIF*.