

May 2020

By Financial Crime Compliance (FCC)

Introduction

Standard Chartered is committed to countering financial crime. This bulletin considers how the COVID-19 pandemic may impact the capabilities of terrorist organisations and lone actors either to raise funds or otherwise benefit from exploiting it. This bulletin aims to raise awareness of potential terrorist financing red flags which may manifest in financial activity.

SUMMARY

- COVID-19 is giving terrorist organisations the chance to raise funds for their activities, most likely through fraud, cyber-crime and diversion, and especially by exploiting charitable giving at a time when donations are increasing
- Extremist groups are adapting their anti-western rhetoric to take advantage of the fear and confusion caused by COVID-19-related unemployment and disillusionment with governments, to increase radicalisation and recruitment
- There is currently no indication of increased active attack planning in the West as a result of the pandemic. High profile 'soft' target opportunities have reduced but the threat may be displaced to government and critical services

What is the financial impact on terrorist activities?

- Terrorism is not a financially motivated crime. Terrorism is often funded and resourced through legitimate means, making terrorist financing (TF) particularly difficult to identify through transactional analysis alone.
- Payments made in support of terrorism may be: **explicit**, e.g. donations to known Large Terrorist Organisation (LTO) affiliated charities or individuals; **clandestine**, e.g. using the cover of purportedly licit fundraising to knowingly contribute to TF; **unwitting**, e.g. payments made in good faith to charitable causes that are diverted by 'bad actors'; or **fraudulent** e.g. using scams to raise revenue for TF, including fake charities.
- There are a number of current COVID-19-related fraudulent criminal activities which may be connected to TF, when evaluated in conjunction with other information:
 - **Fake investments** in COVID-19 related goods and **Fake companies** e.g. posing as suppliers of Personal Protective Equipment (PPE) or mis-selling medical support services.
 - **Fake charity fundraising schemes** e.g. raising money for COVID-19 causes where funds are then misappropriated.
 - **Cyber-enabled COVID-19 themed scams** e.g. using established 'social engineering' techniques to elicit personal or corporate information from individuals to then trick businesses into diverting or rerouting funds into criminally controlled bank accounts.

What is the general impact on terrorist activities?*

- Islamist extremist and right-wing extremist groups are adapting their established anti-western narratives to take advantage of the fear and confusion caused by the pandemic; some propaganda is inciting individuals to use COVID-19 as a 'weapon' to infect others.
- It is likely that unemployment and disillusionment with state apparatus may drive individuals to seek alternative sources of income and ideology, thereby increasing the number of self-radicalised individuals and membership of extremist groups.
- Country 'lockdown' policies have reduced opportunities for in-person radicalisation and recruitment, as recreational activities are curbed. However, this activity has likely been displaced to online forums and communications. Some countries, such as the US, have experienced rising reports in hate crimes targeting Chinese and Asian individuals, which may be fuelled by extremist propaganda.
- Two attacks to date, both in March, are considered to be directly COVID-19 related: an unsuccessful attack on a hospital providing Coronavirus critical care facilities by a right-wing extremist in the US; and an opportunistic domestic attack on government officials meeting to discuss the pandemic by Thai insurgency group Barisan Revolusi Nasional.
- Islamic State has called for its supporters to carry out attacks against overburdened health services, however there is no current indication of increased active attack planning by terrorists in the West.
- Internationally, operational freedom for Islamist extremists is increasing in some locations, such as Iraq, due to the withdrawal of military personnel in response to the pandemic. Terrorist groups operating in developing countries, however, are likely to suffer casualties from the virus, particularly those more integrated in communities and public services, disrupting their regular operations.

*Sources: Jane's, US Department of Homeland Security, ABC News, Wall Street Journal


You can find more analysis from Standard Chartered on the impact of the COVID-19 pandemic on criminal activity, on our public website [here](#)

Potential indicators of suspicious financial activity connected to the COVID-19 pandemic


The indicators below should be read in conjunction with all available guidance on fraud and financial crime ‘red flags’. They should also be evaluated in the context of the normal and expected activity of the client or customer, and other available information, to determine if the activity identified meets any reporting thresholds for ‘suspicion’.

Business, Commercial and Corporate & Institutional Banking Scenarios


- Extremist groups and affiliated or connected **charities** (e.g. through corporate ownership) may openly solicit funds for purported charitable causes, with the intention to use the funds raised to finance terrorist activities. Newly formed entities in particular may be created by terrorist fundraisers for this purpose, anticipating that their front status may not be detected by organisations and individuals occupied with responding to the pandemic.

 Company/charity appears to be newly incorporated, especially those with COVID-19 related terms in the company name

- LTO-connected charities may receive more funding from public services, other Non-Profit Organisations (NPOs) and private donors during times of crisis. They are usually locally based in LTO locations.


 Unusual or high levels of cash withdrawals made by NPOs in high risk locations

- Legitimate international NPOs and small charities based in high-risk countries (conflict or humanitarian crisis areas where LTOs are present) may also become more vulnerable to unintended TF as cash is more susceptible to diversion by bad actors.


 Transfers made by NPOs to previously unconnected charitable entities in high risk locations and/or using untested or unverified third parties to do so


Retail Individual Banking Scenarios

- Whilst there are a large number of legitimate charity fundraising initiatives currently active, some individuals may be operating scams to raise funds for terrorist activity and receiving funds collected into their personal bank account.
- Online platforms are likely to be the medium of choice for clandestine or fraudulent (front) fundraising by individuals and small groups, but cash-based donations may also occur. Previously, fraudulent payee organisations have been seen to use a similar but not identical name to that of a reputable charity in order to trick donors.

 Unusual deposits into accounts connected to COVID-19-related charities or crowd-funding, especially where deposits are made from accounts belonging to online platforms

- The convergence between terrorist activity and financial fraud may also increase: there are increased numbers of susceptible individuals active online, increasing targeting opportunities and criminal motivation to exploit the situation.
- Fraudulent scams may include those relating to fake investments in medical supplies or equipment, as well as other forms of cyber enabled fraud (such as phishing).

 Retail individual accounts receive deposits from previously unconnected counterparties (individuals or entities), particularly where they are rapidly disbursed to other accounts, or are withdrawn immediately

 Unexplained increase in account turnover of Retail accounts, particularly where this includes an increase in cash deposits and/or cash withdrawals

Known high risk characteristics associated with **Non-Profit Organisations** and Terrorist Financing:

- More likely to be a service-style NPO (e.g. healthcare)
- High cash intensity
- Public donations are the main source of funds
- Support a particular ethnicity or religion
- Based in provincial or capital cities
- Operate in or send funds to a high-risk country
- Limited visibility of the full funding cycle

[Source: AUSTRAC SE Asia study 2018]

CASE STUDY | An Australia-based charity – which has since been linked to Al Qaida and promoted by Islamic State – issued a 2020 Ramadan fundraising campaign to assist widows and orphans in the Philippines, expressing urgency due to the spread of the virus.

The campaign may benefit from increased levels of community altruism resulting from the pandemic, and potential temporary decreased scrutiny by the authorities. Whilst some of the funds may be used to legitimately help those in need, fund usage for terrorist activity cannot be precluded.

[Source: SITE Intelligence Group]