Following the Christchurch terrorist attacks on 15 March, New Zealand's national threat level has been high. Police is maintaining strong preventative measures in relation to any copycat or retaliation incidents rather than a specific threat.

Implications of threat level for reporting entities

The possibility of copycat or retaliatory attacks raises the likelihood that terrorism financing will be used to raise, move or use funds for terrorist purposes in New Zealand. In particular:

- Domestic financing is more likely to relate to small scale support of small cells or lone actors; and
- Overseas experience indicates that such terrorist operations are more likely to be either self-funded, may receive financial support from close associates, or in some cases may be funded by small payments from international networks.

While the likelihood of such terrorism financing has increased with the change in threat level, this is largely the same likely scenario as before the Christchurch attack. Although financing such operations generally requires relatively small values of funds, they have the potential to cause significant harm to the community.

The small and mundane value of transactions make this type of terrorism financing difficult to detect. However, vigilant application of know your customer processes, account monitoring and suspicious activity reporting (SAR) can help to detect suspicious patterns of activity that can assist authorities.

Obligations

SARs must be submitted when a reporting entity has facts and observations that objectively give reasonable grounds for suspicion that the activity may be relevant to investigation. Reporting entities will need to consider the indicators of money laundering and terrorism financing typologies. Information on typologies and indicators are included in the SAR Guideline published on the Police website:

https://www.police.govt.nz/about-us/publication/financial-intelligence-unit-fiu-guideline-suspicious-activity-reports-sar

Importantly, reporting entities do not need to know what offence the suspicious activity may relate for reasonable grounds to form. As such, reporting entities may have reasonable grounds to believe that an activity is suspicious without realising that it is relevant to terrorism financing.

New Zealand also has domestic systems for designating terrorist entities and persons. Reporting entities should be aware of Police and Ministry of Foreign Affairs and Trade advisories. The designation lists are regularly updated and can be found on the Police website: https://www.police.govt.nz/advice/personal-community/counterterrorism/designated-entities

Dealing with designated persons or entities, weapons proliferation, terrorism and terrorism financing are all criminal offences which may give rise to money laundering and a SAR should be submitted in these situations.

If a reporting entity deals with an individual or organisation and there are reasonable grounds for suspicion in relation to property owned or controlled by a designated terrorist entity a Suspicious Property Report (**SPR**) must be completed, as described in section 43 of the Terrorism Suppression Act (TSA). Any SPRs reported to the FIU must contain all the information specified in Schedule 5 to the TSA. In practice, reporting entities use the same

online system for reporting SPRs as if for SARs, specifically SPRs should be filed using the suspicious transaction form in goAML.

Where reporting entities suspect that the reported activity may be relevant to terrorism financing, they are asked to tick the terrorism financing indicator in goAML and note reason for suspicion that the activity is suspected to be relevant to terrorism financing or property is owned or controlled by designated entity.

Upcoming changes to guidance

The National Risk Assessment found that terrorism financing of significant value is more likely to be associated with overseas terrorism. This assessment remains. However, the change in the national security threat rating raises concern relating to the possibility of small scale financing of domestic terrorism. The public version of the NRA will be updated to include more information on domestic terrorism financing.

The red flag indicators outlined in the FIU SAR Guideline may assist reporting entities to detect suspicious activity should it arise. These indicators are included below. Notwithstanding the change in the National Threat level these indicators remain relevant and are based on international experience of similar terrorist threats.

The FIU is currently working on a more detailed typology report which will be published as soon as possible. Reporting entities may also refer to reporting by the FATF and RUSI on terrorism financing by lone actors and small cells.

SAR Guideline indicators relating to terrorism financing, weapons proliferation and security

- Customer is a person subject to New Zealand sanctions, or is a representative of sanctioned persons or entities.
- Customer accesses accounts, and/or uses debit or credit cards in high risk jurisdictions (including cities or districts of concern), specifically countries (and adjacent countries) under conflict and/or political instability, subject to sanctions, or known to support terrorism activities and organisations.
- Customer identified by media or law enforcement as having travelled, attempted/ intended to travel to high risk jurisdictions (including cities or districts of concern), specifically countries (and adjacent countries) under conflict and/or political instability or known to support terrorism activities and organisations.
- Customer conducted travel-related purchases (for example, purchase of airline tickets, travel visa, passport, etc.) linked to high risk jurisdictions (including cities or districts of concern), specifically countries (and adjacent countries) under conflict and/or political instability or known to support terrorism activities and organisations.
- The customer mentions that they will be travelling to, are currently in, or have returned from, a high risk jurisdiction (including cities or districts of concern), specifically countries (and adjacent countries) under conflict and/or political instability or known to support terrorism activities and organisations.
- Customer depletes account(s) by way of cash withdrawal.
- Customer or account activity indicates the sale of personal property/ possessions.
- Individual/ Entity’s online presence supports violent extremism or radicalisation.
- Customer indicates planned cease date to account activity.
- Customer utters threats of violence that could be of concern to National Security/ Public Safety.
- Sudden settlement of debt(s) or payments of debts by unrelated third party (ies).

- Law enforcement indicates to reporting entity that the individual/ entity may be relevant to a law enforcement and/or national security investigation.
- Customer's transactions involve individual(s)/ entity (ies) identified by media or law enforcement as the subject of a terrorism financing or national security investigation.
- Customer donates to a cause that is subject to derogatory publicly available information (crowdfunding initiative, charity, NPO, non-governmental organisation etc.).
- Customer conducts uncharacteristic purchases (for example, camping/ outdoor equipment, weapons, ammonium nitrate, hydrogen peroxide, acetone, propane, etc.).
- Customer trades in commodities that may also be dually used in missiles, and chemical, biological and nuclear weapons.
- A large number of email transfers between customer and unrelated third party (ies).
- Customer provides multiple variations of name, address, phone number or additional identifiers.
- The sudden conversion of financial assets to a virtual currency exchange or virtual currency intermediary that allows for increased anonymity.