Financial Transactions and Reports Analysis Centre of Canada
Centre d'analyse des opérations et déclarations financières du Canada
Canada

OPERATIONAL ALERT

Reference : FINTRAC-2022-OA002
December 2022

Terrorist Activity Financing

Purpose

The purpose of this Operational Alert is to support reporting entities in recognizing financial transactions suspected of being related to terrorist activity financing. Through financial transaction reports, FINTRAC is able to facilitate the detection, prevention and deterrence of all stages of money laundering (placement, layering and integration) and the financing of terrorist activities by providing actionable financial intelligence disclosures to law enforcement and national security agencies. This Operational Alert provides terrorist activity financing indicators as a result of the analysis of FINTRAC disclosures related to terrorist activity financing.

Background

Terrorist financing provides funds for terrorist activity. Terrorists use techniques like those of money launderers (e.g., structuring, use of nominees) to evade authorities' detection and to protect the identity of their sponsors and of the ultimate beneficiaries of the funds. Like money laundering, funds for terrorist activity financing can be sourced from criminal sources (e.g., drug trade, smuggling of weapons and other goods, fraud, kidnapping and extortion). However, unlike money laundering, funds can be raised from legitimate sources too (e.g., personal donations and profits from businesses and charitable organizations), making the detection and tracking of these funds more difficult. Funds for terrorist activity financing also tend to be in smaller amounts compared to funds in money laundering.

The Government of Canada groups terrorist threats faced by Canada into three broad types of violent extremism: religiously motivated violent extremism (RMVE), politically motivated violent extremism (PMVE) and ideologically motivated violent extremism (IMVE).

Currently, 77 terrorist entities are listed under the *Criminal Code* and can be found on the Public Safety Canada website. These listings of terrorist entities help safeguard Canada's financial system from furthering terrorist activity by providing the means to seize/ restrain and/or obtain the forfeiture of property belonging to a listed entity. The newest listed terrorist entities since 2019 have included IMVE-related groups – the first time such groups have been listed in Canada.

The Government of Canada states RMVE, PMVE and IMVE all represent a threat to the security of Canada, and IMVE has grown in presence within Canada in recent years. Since 2014, the Government of Canada notes that Canadians motivated in whole or in part by extremist ideological views have killed and wounded more people on Canadian soil than RMVE or PMVE.

The Government of Canada explains types of violent extremism as:

- RMVE encourages the use of violence as part of a spiritual struggle against a perceived immoral system. Followers believe that salvation can only be achieved through violence.
- PMVE encourages the use of violence to establish new political systems, or new structures and norms within existing systems.
- IMVE is often driven by a range of grievances and ideas from across the traditional ideological spectrum. The resulting worldview consists of a personalized narrative which centres on an extremist's willingness to incite, enable and or mobilize to violence. Extremists draw inspiration from a variety of sources including books, images, lectures, music, online discussions, videos and conversations. These individuals and cells often act without a clear affiliation to a specific organized group or external guidance, but are nevertheless shaped by hateful voices and messages online that normalize and advocate violence.

Source: *CSIS Public Report 2020*

Overview of FINTRAC's analysis of disclosures related to terrorist activity financing

FINTRAC analyzed a sample of disclosures from January 2019 to October 2022 related to terrorist activity financing. Based on FINTRAC's analysis, the transactions disclosed fell into three main themes: domestic terrorism, financing international terrorist groups, and Canadian extremist travellers (CETs). All three types of violent extremism, as identified by the Government of Canada, were observed in FINTRAC's sampled disclosures, with IMVE and RMVE being the most common.

FINTRAC analyzed its disclosures from the past two years associated to terrorism threats specifically occurring in Canada—that is, the target of terrorism was in Canada (regardless if a terrorism event actually occurred) and is in-line with what Public Safety Canada refers to as domestic terrorism incidents and threats in the Federal Terrorism Response Plan. Among these FINTRAC disclosures, most were related to IMVE. Based on FINTRAC's analysis, IMVE actors in Canada fell into three sub-categories: lone actors, cross-border networks and organized groups. Lone actors tended to be self-funded, often by payroll, government assistance deposits, and/or cash deposits. Cross-border networks mainly used large money services businesses (MSBs) to transfer funds, along with electronic money transfers (EMTs). These funds were mainly sent to third parties, often in locations of concern for IMVE activity[1]. Organized groups raised funds through a variety of methods, including EMTs, sales of merchandise, and frequent cash deposits. The reference section of EMTs often included particular words, phrases and/or numbers (e.g., years of particular significance to their ideology or numbers that correspond to the group's name) that linked the transaction to a particular IMVE group. FINTRAC's analysis revealed that IMVE financing activity involved actors located and operating in Canada. While there were funds being sent overseas to suspected IMVE actors, based on financial transactions analyzed, there were IMVE operations/activities being organized within Canada as well.

FINTRAC found that transactions relating to the financing of international terrorist groups consisted primarily of outgoing funds transfers to another country – particularly to jurisdictions of concern for terrorist activity financing[2]. The jurisdictions of concern most frequently seen in the sampled FINTRAC disclosures included: Iraq, Lebanon, Pakistan, Syria, Turkey, United Arab Emirates, and Yemen. These outgoing international fund transfers, often funded by cash deposits, were conducted by individuals in Canada and primarily involved the use of MSBs.

Within the analyzed disclosures, the most frequently identified international terrorist entity was Daesh, followed by Hizballah. A large portion of the funds suspected of supporting Daesh were sent to Turkey, often to regions or towns close to the Turkey-Syria border, a particular high risk region for terrorist activity financing.

A large portion of funds suspected of funding Hizballah were sent to Lebanon. Funds suspected of funding Hizballah were frequently sent or received by individual/entities referencing sale of cars or listed in the automotive industry.

FINTRAC continues to receive suspicious financial transactions related to the threat of Canadian extremist travellers (CETs). The five phases of CETs identified in FINTRAC's 2018 Terrorist Financing Assessment remain relevant and were observed in the financial transactions analyzed. The five phases are: Pre-departure, En Route, In Theatre, Returning, and Interrupted travel. FINTRAC observed that CETs in the Pre-departure phase often depleted their accounts prior to travel by way of cash withdrawals. A significant shift from historic account activity was also observed in the accounts of CETs prior to departure from Canada. Individuals in the En Route phase often demonstrated financial activity that included the use of debit or credit cards along known travel corridors to a conflict zone or location of concern. Often, accounts were dormant while the CET is in the In-theatre phase. Use of these accounts would then resume upon the CET's return to Canada. Additionally, CETs returning to Canada frequently sent and/or received international transfers and received cash deposits from third parties with no clear purpose. The travel of aspiring CETs was sometimes interrupted before they were able to leave Canada. According to publicly available information, this was due to intervention by law

Canada

enforcement. Among the sampled FINTRAC disclosures, travel-related refunds, such as airline tickets, often occurred in accounts of these disrupted travellers.

Reasonable grounds to suspect and how to use indicators

How reporting entities determine if they submit a suspicious transaction report to FINTRAC (for either a completed or attempted financial transaction) requires more than a "gut feel" or "hunch," although proof of terrorist activity financing is not required. Reporting entities are to consider the facts, the context and terrorist activity financing indicators of a transaction. When these elements are viewed together, they create a picture that is essential to differentiate between what may be suspicious and what may be reasonable in a given scenario. Reporting entities must reach reasonable grounds to suspect that a transaction, or attempted transaction, is related to terrorist activity financing before they can submit a suspicious transaction report to FINTRAC.

Indicators of terrorist activity financing can be thought of as red flags indicating that something may very well be wrong. Red flags typically stem from one or more characteristics, behaviours, patterns and other contextual factors related to financial transactions that make them appear inconsistent with what is expected or considered normal. On its own, an indicator may not initially appear suspicious. However, it could lead reporting entities to question the legitimacy of a transaction, which may prompt them to assess the transaction to determine whether there are further facts, contextual elements or additional money laundering (ML) or terrorist financing (TF) indicators that would increase their suspicion to the point where submitting an STR to FINTRAC would be required (see FINTRAC Guidance on Suspicious Transaction Reports).

Reporting Terrorist Property to FINTRAC

Reporting entities must submit a terrorist property report (TPR) to FINTRAC under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* and associated regulations when they are required to make a disclosure under section 83.1 of the *Criminal Code* or under section 8 of *the Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism*. A disclosure is required in the following situations: (a) when reporting entities know of the existence of property in their possession or under their control is owned or controlled by or on behalf of a terrorist or a terrorist group; and (b) when reporting entities have information about a transaction or proposed transaction in respect of property owned or controlled by or on behalf of a terrorist or a terrorist group.

For the purposes of the disclosure described above, property is anything owned or controlled by a person or entity, whether tangible or intangible. It includes real and personal property of every description, as well as deeds and instruments that give a title or right to property, or a right to recover or receive money or goods. It also includes any property that has been converted or exchanged, or that has been acquired from any conversion or exchange. Examples of property include cash, monetary instruments, casino products and tokens, virtual currency, bank accounts, prepaid payment products and prepaid payment product accounts, securities, jewellery, precious metals or precious stones, real estate, and insurance policies. Therefore, when such property is owned or controlled by or on behalf of a terrorist or a terrorist group, and is in the possession or under the control of a reporting entity, or a reporting entity has information about a transaction or proposed transaction in respect to such property, the reporting entity must make a disclosure to the RCMP or CSIS and submit a TPR to FINTRAC.

TPRs differ from other reports submitted to FINTRAC because a transaction or attempted transaction does not need to occur for reporting entities to submit a TPR. Instead, the mere existence of property owned or controlled by or on behalf of a terrorist group or information about a transaction or proposed transaction in respect to such property, prompts reporting entities' obligation to disclose to the RCMP or CSIS, and submit a TPR to FINTRAC. If a transaction was attempted or completed involving the property that reporting entities know is owned or controlled by or on behalf of a

terrorist or a terrorist group, then reporting entities should also submit an STR to FINTRAC. For clarity, if reporting entities are not sure but suspect that the property in their possession or control is owned or controlled by or on behalf of a terrorist or a terrorist group, then reporting entities must submit an STR to FINTRAC if there was an attempted or completed transaction associated with this property.

Reporting entities must submit a TPR to FINTRAC immediately once they are required to make a disclosure under the *Criminal Code* or the Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism. For more information on submitting a TPR, please see Guidance on Reporting Terrorist Property to FINTRAC.

Terrorist Activity Financing Indicators

Below are indicators related to terrorist activity financing derived from FINTRAC's analysis and reflect the types and patterns of transactions, along with contextual factors, which emphasize the importance of knowing your client. Indicators from FINTRAC's money laundering and terrorist financing indicators – financial entities and FINTRAC's Terrorist Financing Assessment 2018 are included below as they remain relevant and should be considered all together.

These indicators should not be treated in isolation; on their own, these indicators may not be indicative of terrorist activity financing or other suspicious activity. They should be assessed by reporting entities in combination with what they know about their client and other factors surrounding the transactions to determine if there are reasonable grounds to suspect that a transaction or attempted transaction is related to the commission or attempted commission of a terrorist activity financing offence. Several indicators may reveal otherwise unknown links that, taken together, could lead to reasonable grounds to suspect that the transaction or attempted transaction is related to the financing of activity related to the commission or attempted commission of a terrorist activity financing offence. It is a constellation of factors that strengthen the determination of suspicion. These indicators aim to help reporting entities in their analysis and assessment of suspicious financial transactions.

Indicators of terrorist activity financing in relation to domestic terrorism

The following indicators are applicable to various types of violent extremism (e.g., IMVE, RMVE, PMVE). Some that are specific to IMVE are in-line with the characteristics identified in FINTRAC's Special Bulletin on Ideologically Motivated Violent Extremism.

- ⊗ Media or law enforcement information linking individual to violent extremist group(s), sentiments or violent extremist activity.
- ⊗ Individual's online presence expresses ideologically motivated violent extremism (IMVE) sentiments or support for a particular IMVE group.
- ⊗ Individual's online presence indicates individual's intent to engage in violent extremist activity e.g., social media post, tweet, hashtag, and/or manifesto.
- ⊗ Subjects are involved in transactions with individuals, groups, clubs, businesses and/or charities who have been associated with violent extremist groups by the media or law enforcement.
- ⊗ Transaction details (contact name, email address, funds totals, remittance info etc.) makes references to words, phrases and/or numbers linked to violent extremist actors, groups, activity, or iconography.
- ⊗ Payments/transfers with no clear link between sender and receiver are made to high risk jurisdictions known or suspected for IMVE activity.
- ⊗ Excessive email money transfers followed by the depletion of funds through third parties or cash withdrawals.
- ⊗ Purchases, travel expenses or irregular account activity leading up to and/or in areas where violent extremist activity has occurred.

Canada

- ⊗ Client conducts purchases at vendors who sell firearms, fire-arm making kits, ammunition, explosives, and/or tactical gear.
- ⊗ Payments to online retailers, charities, individuals or businesses that are known, or believed to sell violent extremist paraphernalia, literature and/or merchandise.
- ⊗ Payments to online gaming platforms, particularly platforms with in-platform chat rooms that are known to be frequented by violent extremist groups.
- ⊗ Monthly and/or one time payments are made to extremist media outlets and/or propaganda websites.
- ⊗ Individual/ entity facilitating and/or selling merchandise, tickets, and/or donations that may be linked to violent extremist groups.
- ⊗ Email money transfers, cheque deposits, online payment service deposits and/ or cash deposit transferred on a monthly basis which lacks any explicit business or economic purpose, often in low dollar amounts, for the suspected purpose of membership fees.
- ⊗ Transaction details make reference to membership fees or clubhouse fees.
- ⊗ Use of crowdfunding, FinTech platforms and/or cryptocurrencies to finance individuals or groups associated with violent extremism.
- ⊗ Transactions involving an individual or entity linked to hate crime(s) or hate speech.
- ⊗ Individual receives payments/direct deposits from livestream platforms that accept donations.

Indicators of terrorist activity financing in relation to support of international terrorist groups

Some of the following indicators were also included in FINTRAC's Guidance on money laundering and terrorist financing indicators – financial entities. They continue to be commonly reported indicators observed by FINTRAC in suspicious terrorist activity financing transactions.

- ⊗ Transactions involving certain high-risk jurisdictions; such as locations in the midst of or in proximity to, armed conflict where terrorist groups operate or locations which are subject to weaker ML/TF controls.
- ⊗ Client receives excessive email money transfers (EMTs) and/or cash deposits, not in line with stated occupation, and are used in part to fund wires to a high-risk jurisdiction and/or cash withdrawals within a short period of time.
- ⊗ Sending or receiving international transfers to and/or from locations of specific concern.
- ⊗ An account opened in the name of an entity, a foundation or association, which may be linked or involved with a suspected terrorist groups.
- ⊗ The use of funds by a non-profit organization is not consistent with the purpose for which it was established.
- ⊗ Raising donations in an unofficial or unregistered manner.
- ⊗ Transactions involve persons or entities identified by media and/or sanctions lists as being linked to a terrorist group or terrorist activities.
- ⊗ Law enforcement information provided which indicates persons or entities may be linked to a terrorist group or terrorist activities.
- ⊗ Individual or entity's online presence supports violent extremism or radicalization.
- ⊗ Individual donates to a cause that is the subject of derogatory information that is publicly available (e.g. crowdfunding initiative, charity, non-profit fundraiser, etc.).
- ⊗ Transactions involving businesses involved in auto sales or automobile shipping in an area of concern, sending funds to similar types of companies or to individuals where the purchasing of cars is referenced.
- ⊗ Non-profit or charitable organizations conduct financial transactions (e.g., large cash deposits or wire transfers to location of concern) that does not appear to be in line with stated activity of the organization.

- ⊗ Individual sends and/or receives wire transfers to/from a number of individuals in different countries without an apparent purpose.

Indicators of terrorist activity financing in relation to Canadian Extremist Travellers (CETs)

Some of the following indicators were included in FINTRAC's 2018 Terrorist Financing Assessment. They continue to be commonly reported indicators observed by FINTRAC in suspicious terrorist activity financing transactions.

Pre-Departure

- ⊗ Individual indicates planned cease date to account activity.
- ⊗ Individual or account activity indicates sale of personal possessions.
- ⊗ Purchase or airline ticket to country in the vicinity of a conflict zone.
- ⊗ Use of funds for other travel-related items (e.g. purchase at passport office).
- ⊗ Donations to non-profit organizations linked to terrorist financing activity.
- ⊗ Use of funds from social assistance, student loans or other credit products ("debt financing").
- ⊗ Exploitation of available credit products, including maxing out credit cards (often via cash advances), not making payments and transferring balance to personal debit account.
- ⊗ Depleting account via cash withdrawals.
- ⊗ Account activity shows a significant shift from historical activity in account.

En-Route

- ⊗ Client notifies reporting entity of travel to a third country via a country contiguous to a conflict zone, but subsequent financial activity indicates the journey was not completed.
- ⊗ Financial activity, such as debit or credit card usage, along a known travel corridor to a conflict zone or location of concern.
- ⊗ Client accesses or attempts to access their online banking from inside or along the border of a conflict zone.
- ⊗ Receipt of funds transfers inside or along the border of a conflict zone.
- ⊗ Purchases for prepaid SIM cards and/or prepaid data plans.

In Theatre

- ⊗ Individual receives money transfers from family or friends in or in the vicinity of a conflict zone.
- ⊗ Publicly available information and media indicates that the individual has travelled to a conflict zone.
- ⊗ Client accounts go dormant.

Returning

- ⊗ Individual reinitiates activity on a dormant account.
- ⊗ Individual begins receiving new sources of income (e.g. employment, social assistance).
- ⊗ Individual sends or receives atypical domestic or international transfers.

Disrupted travel

- ⊗ Individual made travel-related purchases, such as of airline tickets or a visa, which were subsequently refunded.
- ⊗ Individuals indicated they would be travelling out of the country but transaction history suggests the travel did not occur.
- ⊗ Publicly available information indicates that the individual was prevented from travelling for security reasons.

Canada

Contact FINTRAC

Email: guidelines-lignesdirectrices@fintrac-canafe.gc.ca
Telephone: 1-866-346-8722 (toll-free)
Facsimile: 613-943-7931
Mail: FINTRAC, 24th Floor, 234 Laurier Avenue West, Ottawa ON K1P 1H7, Canada

Cat. No. FD4-27/2022E-PDF
ISBN 978-0-660-41873-5

Canada

Resources

For more information on terrorist activity financing, violent extremism as well as associated financial intelligence, please consult the following resources:

Canada

- CSIS: "*Public Report 2020*"
- FINTRAC: "*Counter-Terrorist Financing e-Learning Module*" (developed in partnership with the Egmont Centre of FIU Leadership and Excellence)
- FINTRAC: "*Special Bulletin on Ideologically Motivated Violent Extremism: A Terrorist Financing Profile*"
- FINTRAC: "*Terrorist Financing Assessment 2018*"
- Public Safety Canada: "*Currently Listed Entities*"

International

- Egmont Group-Information Exchange Working Group: "*Counter Terrorist Financing Project-Lone Actors and Small Cells*"
- Federal Bureau of Investigation/National Counterterrorism Center, and the Department of Homeland Security (United States): "*Homegrown Violent Extremist Mobilization Indicators (2019 Edition)*"
- Financial Action Task Force: "*Ethnically or Racially Motivated Violent Terrorist Financing*"
- Financial Action Task Force: "*Risk Assessment Guidance on Terrorist Financing*"

[1] High risk jurisdiction in this context may include Eastern Europe or other geographic region where the IMVE group in question is known to operate.

[2] Jurisdictions of concern are identified by several factors including if listed terrorist entities are known to operate or jurisdiction with identified deficiencies relating to the implementation/enforcement of anti-terrorist financing measures. Refer to FINTRAC's Terrorist Financing Assessment 2018 for more details on jurisdictions of concern relating to terrorist activity financing.

Canada