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

Reference number: 2021-SIRA-001
July 2021

Special Bulletin on Ideologically Motivated Violent Extremism: A Terrorist Activity Financing Profile

In February 2021, the Government of Canada added four ideologically motivated violent extremism (IMVE) organizations to the *Criminal Code* list of terrorist entities. In June 2021, the Government of Canada added three more IMVE entities to that list: two organizations and one individual. Reporting entities should be aware of these new listings, as well as observed patterns in the financing behaviour of IMVE threat actors[1].

The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) continues to support reporting entities by producing strategic intelligence products that provide analytical perspectives on the nature, scope and threats posed by money laundering and terrorism financing. To that end, this Special Bulletin presents the results of FINTRAC's analysis of IMVE-related transaction reporting, supplemented by information from media reports and academic research.

Introduction

IMVE in Canada is driven by a range of grievances that transcend the traditional left–right ideological spectrum. IMVE is also distinct from religiously motivated violent extremism (RMVE) and politically motivated violent extremism (PMVE). The Canadian Security Intelligence Service has divided the violence carried out by threat actors associated with IMVE in Canada into four categories:

- *xenophobic violence*: racially or ethnically motivated violence based on fear or hatred of what is perceived to be foreign, strange or different;
- *anti-authority violence*: violence against the authority of state and law-enforcement entities;
- *gender-driven violence*: violence motivated by hatred of those with a different gender or sexual orientation; and
- *other grievance-driven and ideologically motivated violence*: violence committed by individuals with no clear association with an organized group or any external guidance.

[1] Considering the complex and diffuse nature of the IMVE threat landscape, threat actors could include individuals, cells, groups, networks, and platforms.

Background[2]

The terrorism threats posed by IMVE threat actors are on the rise around the world. According to a 2020 Trends Alert report published by the United Nations Counter-Terrorism Committee Executive Directorate, there has been a significant rise in terrorist attacks with links to extreme right-wing movements and ideologies[3] over the last five years.

In 2019, Blood and Honour and its armed branch, Combat 18, were the first two IMVE-related organizations to be included on the *Criminal Code* list of terrorist entities. In February 2021, the Government of Canada added four IMVE organizations to this list: Proud Boys, Atomwaffen Division, The Base and Russian Imperial Movement. In June 2021, Three Percenters, Aryan Strikeforce and American neo-Nazi James Mason were also added to this list of terrorist entities.

Violence in Canada that was motivated in whole or in part by IMVE has tended to take the form of spontaneous arsons, assaults and homicides. Targets include people of the Islamic and Jewish faiths, people of colour, women, Indigenous peoples and members of LGBTQ2+ communities. Examples of recent IMVE attacks in Canada include the Quebec City mosque attack in 2017, the Toronto van attack in 2018, and the Toronto spa attack in 2020. This last instance saw, for the first time in Canada, terrorism charges brought against an individual associated with an IMVE ideology.

IMVE threat actors in Canada thrive online as the Internet allows these actors to connect anonymously across borders. IMVE threat actors in Canada use the Internet to make targeted calls for attacking equity-deserving groups offline, and to perpetuate racist and misogynistic tropes on social media that feed into broader narratives associated with conspiracy theories and anti-government movements.

Lone actors in the global IMVE context—those who, by themselves, carry out or attempt to carry out violent attacks in their home country or travel to possibly take part in violent activities elsewhere—raise their own funds, using their savings, employment income or money from family and friends.

Internationally, IMVE threat actors have raised funds through commercial activities, such as selling merchandise, holding events such as talks and concerts, crowdfunding, charging membership fees and accepting donations. IMVE threat actors have also been known to turn to drug trafficking, weapons trafficking and robberies to fund their operations. IMVE threat actors use the funds raised to recruit new members, engage in day-to-day activities and carry out promotional efforts such as making videos. In addition, the funds go toward organizing marches and events, maintaining websites, paying the legal fees of individuals arrested for their involvement in the IMVE movement, acquiring weapons and establishing safe houses.

In recent years, online crowdfunding platforms and social media sites have started to crack down on IMVE fundraising and promotional activities. This has led IMVE threat actors to seek alternative outlets. These tend to be smaller platforms than the mainstream ones, and they do not always have the resources to monitor and shut down IMVE activities. In response to increased restrictions on online platforms, IMVE threat actors have been encouraging their followers to send them money via mail, cheques or money orders. Following their de-platforming, IMVE threat actors have also increasingly turned to virtual currencies for fundraising. Threat actors mainly use virtual currency donations to

[2] This section relies on open source, academic and external reporting to provide the context in which terrorist activity financing related to IMVE occurs.
[3] As per the Government of Canada definition, these groups would fall under the IMVE category that is the subject of this publication.

fund their propaganda and recruitment efforts. The use of virtual currency has been associated with only one IMVE attack so far.

Observations in suspicious transaction reporting

FINTRAC observed a number of key patterns in IMVE threat actors when analyzing reporting that contained a reference to IMVE-related activity.[4] Overwhelmingly, this data highlights general suspicions of terrorist activity financing and money laundering, particularly of the proceeds of drug-related crimes. The majority of IMVE-related financial transactions were concentrated in Alberta, British Columbia and Ontario.

Lone actors

The financial behaviour of lone IMVE actors is similar to that of lone actors in the RMVE space. Lone actors primarily used personal funds, such as those received from employment income or family members, to carry out attacks. There was no indication in the reporting that the family members were aware that the funds would be used for violent action.

As such, lone actors may be difficult to identify through transactions patterns or financial activity alone. Lone actors commonly used electronic money transfers to both send and receive funds, made cash withdrawals, and carried out regular debit and credit activity to send funds. Further, many lone actors were observed to have sent money transfers to unknown third parties. Lone actors were also observed using their own funds to buy weapons, either through online chain stores or in person. These individuals also carried out routine debit and credit account activity.

Cross-border networks

Individuals in Canada may fund international IMVE networks, while not necessarily being members of organized groups themselves. These individuals typically used payment processing companies and money services businesses to make international funds transfers. While these transactions tended to be small, recurring transfers to multiple nodes of the same international network in different countries, they totalled significant amounts. Financial support to IMVE threat actors also took the form of one-time donations.

Funds were typically sent to pay membership fees, purchase merchandise and gear, and to make general donations to IMVE threat actors overseas. Additionally, some of the beneficiaries forwarded the funds to recruiters for far-right militias and other similar groups. FINTRAC observed that Canadians were most often senders, not recipients, of funds.

Organized threat actors

Organized IMVE threat actors in Canada use both personal and business accounts to conduct their financial activities. Personal and business account transactions showed connections between IMVE threat actors, and individuals and companies charged with crimes such as fraud, robbery, assaulting police officers, drug trafficking and weapons offenses.

Using personal accounts, IMVE threat actors largely relied on electronic money transfers and cash deposits for their fundraising activities. These transfers typically involved small amounts. The majority of funds were suspected to be used to buy firearms and gear, as well as for donations and membership fees. FINTRAC observed several IMVE-related payments to personal accounts from crowdfunding sites.

[4] These transaction reports predate the additions of new IMVE-related entities to the list of terrorist entities in February and June 2021.

FINTRAC is aware of the growing use of virtual currencies by IMVE threat actors to send and receive funds. However, the individuals conducting transactions with someone in the network of IMVE threat actors were not always IMVE threat actors themselves.

The continued use of business accounts by IMVE-related actors could enable groups to raise larger amounts of funds under the guise of legitimate business transactions. This is because business transactions are generally larger than those involving personal accounts and can be conducted without raising much suspicion.

Characteristics in the financing of IMVE activity

The broad characteristics of IMVE found in suspicious transaction reports set out below may not necessarily be indicative of terrorist financing. Consequently, reporting entities must examine them in conjunction with additional risk indicators. These include transactions with links to IMVE threat actors listed as terrorist entities or adverse media reporting.

Personal account activity

— Absence of expected personal transactions such as normal debit and credit account activity and/or paying bills
— Sudden cessation of personal activity
— Numerous and frequent electronic money transfers followed by the depletion of funds through transfers to third parties

Business account activity

— Absence of regular salary payments and business-related activity, except insurance and loan payments
— Funds received from and sent to unrelated businesses that do not align with the client's business profile
— Absence of business-related purchases

Reporting to FINTRAC

To facilitate FINTRAC's disclosure process, please include the term **#IMVE** in the Part G-Description of suspicious activity of the Suspicious Transaction Report if applicable. For guidance on submitting suspicious transaction reports to FINTRAC, see Reporting suspicious transactions to FINTRAC.

Contact FINTRAC

- **Email**: guidelines-lignesdirectrices@fintrac-canafe.gc.ca (include Special Bulletin 2021-SIRA-001 in the subject line)
- **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. FD4-25/2021E-PDF
ISBN 978-0-660-38039-1

FINTRAC Special Bulletins provide information related to new, emerging and particularly topical methods of money laundering and terrorist activity financing. However, these Bulletins should not be considered legal advice. Please refer to the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* and its associated Regulations for the full description of the reporting entities' obligations.