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

FINTRAC-2026-SB002
April 2026

Special Bulletin on money laundering associated with extortion directed at Canada's South Asian diaspora

Under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (the Act), the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) produces strategic intelligence on the nature and scope of money laundering, terrorist activity financing, sanctions evasion, and the financing of threats to the security of Canada.

This Special Bulletin provides current insights into financial activities related to extortion and targeted violence targeting Canada's South Asian diaspora communities across Canada, particularly in British Columbia, Alberta, Manitoba, and Ontario. The news media is reporting an increase in extortion attempts, shootings, arson attacks and cross-border criminal networks, as well as the involvement of foreign nationals, including organized crime groups with links to India. These activities threaten public safety, undermine community well-being, and create significant financial, operational, and psychological pressures on victims.

Extortion as an evolving threat

Extortion targeting South Asian communities in Canada has evolved from sporadic threats into a sustained campaign of coercion that blends intimidation, opportunistic violence, and trans provincial coordination, with notable concentrations in British Columbia, Alberta, Manitoba, and Ontario. Victims are often small and medium-sized business owners in sectors like retail, transportation, construction, real estate, and hospitality. Extortion events typically begin with anonymous calls or messages over encrypted chat applications demanding large payments, sometimes in the range of hundreds of thousands to millions of dollars. Circumstances escalate to gunfire at homes or storefronts and, in some cases, arson when demands are refused. Police statistics and media reporting reflect the scale and persistence of the problem. Across Brampton, Mississauga, and Caledon authorities logged hundreds of extortion investigations in 2024 and 2025.

The extortion targeting Canada's South Asian diaspora, along with the associated money laundering activities, appears to be primarily associated to loosely organized criminal networks blending local actors with individuals claiming affiliation to overseas organized crime groups. FINTRAC analysis suggests that multiple crime groups appear to be involved in ongoing extortion activities, including the Bishnoi Gang and Bambiha Gang. Notably, reporting submitted to FINTRAC indicates the possibility of "copycat" actors leveraging the weight associated with these crime groups to maximize their own impact.

At an operational level, perpetrators appear to blend low tech coercion with opportunistic use of Canada's financial and communications infrastructure. Phone-based threats and encrypted messaging are common, but offenders also depend on products or services like rental cars and short-term accommodations to stage attacks and quick moving cash couriers or nominees to collect and disperse funds. Suspicious transaction reporting that connects financial activities (such as

The **Bishnoi Gang**, led by Indian gangster Lawrence Bishnoi, is one of the most prominent and violent organized-crime groups originating in northern India. The BISHNOI GANG is a transnational criminal organization with a presence in Canada and is active in areas with significant diaspora communities. The gang's core criminal portfolio reportedly includes a variety of fraud schemes, human trafficking, narcotics trafficking, extortion, and targeted killings, which are described as its largest revenue sources both domestically and abroad. The group operates through a vast network of enforcers and international associates, including collaborators from other Indian crime syndicates, who help coordinate contract killings and other financially motivated crimes from outside India. The BISHNOI GANG creates a climate of insecurity for Canadians in diaspora communities as it targets them, their prominent community members, their businesses, as well as cultural figures within the community. The entity is also known as Bishnoi Group, Lawrence Bishnoi Group, and the Bishnoi Crime Group and was designated by the Government of Canada as a listed terrorist entity on September 29, 2025.

The **Bambiha Gang**, named after deceased leader Davinder Bambiha, functions as a rival to the Bishnoi syndicate and has grown into a sprawling network of operatives involved in extortion, contract violence, and large-scale protection rackets. The organization operates through a multi-layered structure of regional commanders inside India and international coordinators based abroad (including Canada and the U.S.), enabling it to sustain operations ranging from violent attacks to coordinated intimidation campaigns. The gang reportedly forges alliances with other criminal syndicates to expand its influence and revenue streams, particularly in the lucrative extortion economy.

placement, layering, and transmission) with suspected extortion events are of high value to FINTRAC and its partners in law enforcement. This 'footprint of many small and medium business owners' could translate into the following:

- suspicious transaction reporting
- detailed customer interaction notes
- faster information sharing between financial institutions and law enforcement under appropriate legal frameworks

Callers demanding money may identify themselves as part of the Lawrence Bishnoi network, a gang designated as a terrorist organization in Canada, with victims describing threats, shootings, and persistent attempts to collect large payments. These groups appear to recruit or rely on individuals already living in Canada to act as financial intermediaries ("money mules"), enforcers, or "foot soldiers", typically financially vulnerable, young male Indian nationals in Canada on study permits.

The criminal activity appears to be carried out by fluid and interconnected networks rather than isolated actors. Media reports suggest that suspects involved in one set of incidents are often connected to other acts of violence in different locations. This indicates a pattern in which small groups or lone operatives carry out tasks on behalf of larger, loosely organized criminal networks. The mobility of suspects reinforces the assessment that these networks operate across geographic boundaries. This adaptability allows offenders to exploit coordination gaps, making it difficult for authorities to contain their activities.

Overall, extortion directed at South Asian diaspora communities has become a multifaceted threat defined by intimidation, violence, financial coercion, and networked criminal operations that exploit both social dynamics and procedural vulnerabilities. Effective mitigation requires early reporting and strong institutional vigilance. Continued

efforts are also needed to reduce the stigma and fear that prevent victims from seeking help. These are factors that offenders increasingly rely on to maintain their influence and avoid detection.

Financial elements

The financial aspects of extortion illustrate both classic and contemporary patterns. Victims often face immediate demands for lump sum payments through email money transfer, cheques, cryptocurrency, or cash deliveries arranged under duress. FINTRAC analysis suggests that victims negotiate large demands for smaller one-time or reoccurring "payment plans". Some have reportedly liquidated assets or moved capital abroad out of fear for their safety, a reaction that both disrupts local economic activity and interferes with the visibility of funds that might otherwise assist investigative tracing. These shifts, while understandable, can amplify the financial irregularities that accompany coercive crime, making it vital for institutions to maintain heightened awareness of unusual withdrawals, transfers, or spending patterns that coincide with known intimidation trends.

Suspicious transaction reporting pertaining to extortion within South Asian communities suggests money laundering and, potentially, terrorist activity financing abuse across financial entity categories, including financial institutions such as banks and credit unions, money services businesses, including those dealing in virtual currencies, and casinos.

The money-laundering methods used by criminal groups involved in South Asian diaspora-targeted extortion primarily involve substantial cash placement through bank deposits and automated teller machine transactions, as well as heavy layering and flow-through using email money transfers. Suspicious transaction reporting submitted to FINTRAC indicates that individuals implicated in violent extortion activities were observed processing email money transfers, cheques, and cash deposits in volumes and values inconsistent with their reported status, for example, as international students. It also suggests that criminal elements employ nominees and money mules to layer the proceeds of crime and conceal financial source and destination.

Extortion networks rely on financial systems to move proceeds and support operations. Typical financial behaviours include cash collection and informal remittance channels to conceal participants, rapid transfers across provinces aligned with multi-jurisdictional crime groups, use of nominees, relatives, or temporary residents to receive or forward funds.

Typically, extortion demands or protection rackets examined in these cases initially demand hundreds of thousands of dollars to several million dollars from victims. However, email money transfers and cash deposit values analyzed by FINTRAC suggest that individual payments may be within a much lower range: hundreds of dollars to tens of thousands of dollars. It implies that victims probably negotiate with extortionists for payouts to be more realistic or manageable. High value payments may be substituted for "financing plans" that pay enforcers smaller amounts over a set period.

Financial transaction indicators

These indicators should not be treated in isolation. Several indicators may reveal otherwise unknown links that, taken together, could reveal money laundering or terrorist financing activities. Reporting entities should assess indicators in combination with what they know about their client, along with other factors surrounding the transaction 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 money laundering or terrorist financing offence.

- The customer may be referenced in adverse media reports relating to extortion events targeting South Asian communities, as well as to arson, shootings, and murder. Absence of adverse news media in cases where other indicators exist should not deter reporting proactively on suspicious persons or activities.

- The customer may use aliases, pseudonyms or "rapper" stage names. In cases associated with extortion directed at the South Asian diaspora community, the individual will typically be between 17 and 28 years old, possess an Indian passport and have identified as an international student at account creation, generally at a college rather than a university.
- The customer will likely conduct unexplained cash deposits, some of which may be structured and occur at several branch locations, and at automated teller machines. These deposits may finance rapid email money transfers to unknown third parties.
- The customer receives, processes, and transmits an unusual volume of email money transfers that total substantial values that are inconsistent with their status as a student or identified employment. The activity of email money transfers may display many-to-one patterns or funnelling. Some of this activity may appear to be flow-through only.
- The customer uses money services businesses or banks to transact with persons or companies in India, the United Arab Emirates, the United Kingdom, and possibly Portugal or Kenya. Transaction volume or values are likely to be unusually high for their employment status, such as an international student. The customer may also request or receive electronic fund transfers to or from these jurisdictions, including if the sending parties or beneficiaries are in Haryana or Punjab, India.
- The customer may display financial indicators associated with the illegal narcotics trade.
- The customers who are international students may pay for lodging (hotels or short-term rentals), travel booking services, gas or petrol, and fast food in locations subject to extortion activities targeting the local South Asian community and potentially far from the customer's post secondary institution and without persistent prior financial links to those areas.
- Victims of extortion are likely to be a local business owner. The transaction they are seeking to complete, such as a large cash withdrawal or wire transfer, will be inconsistent with past transaction behaviours. The customer may be nervous or distressed and appear to be receiving direction or coaching as they attempt to liquidate long-term investments or execute large or multiple outgoing wires to new counterparties.

Reporting suspicious transactions to FINTRAC

Reporting entities are critical in Canada's anti-money laundering and anti-terrorist financing efforts. Under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act and associated Regulations, reporting entities must submit a suspicious transaction report to FINTRAC if there are reasonable grounds to suspect that a financial transaction that occurs or is attempted is related to the commission or the attempted commission of a money laundering, terrorist financing or sanctions evasion offence.

Operation TAPEX (Timely Analysis of Proceeds from Extortion) is FINTRAC's initiative to support analysis related to proceeds generated by criminals extorting South Asian diaspora communities. To facilitate FINTRAC's disclosure process, please include the term **#TAPEX** in the grounds for suspicion narrative of the Suspicious Transaction Report.

To ensure suspicious transaction reports related to extortion activities are high-quality, reporting entities should:

- identify any suspected victim and suspect counterparty display names, usernames
- identify third parties (e.g., virtual asset service providers) exchanging fiat currency for cryptocurrency; and
- identify relevant customer and counterparty cryptocurrency wallet addresses, where available

Additionally, please see the following links for FINTRAC's risk assessment guidance and compliance requirements.

- Risk assessment guidance
- Compliance program requirements

For guidance on submitting suspicious transaction reports to FINTRAC, see: Reporting suspicious transactions to FINTRAC.

Reporting listed person or entity property to FINTRAC

Reporting entities must submit a listed person or entity property report to FINTRAC under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* and associated Regulations immediately if required to make a disclosure under:

- section 83.1 of the Criminal Code
- an order or regulation made under the United Nations Act
- an order or regulation made under the Special Economic Measures Act
- subsection 7(2) of the Justice for Victims of Corrupt Foreign Officials Act (Sergei Magnitsky Law)

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 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 Royal Canadian Mounted Police (RCMP) or Canadian Security Intelligence Service (CSIS) and submit a listed person or entity property report to FINTRAC.

Listed person or entity property reports differ from other reports submitted to FINTRAC because a transaction or attempted transaction does not need to occur for reporting entities to submit a listed person or entity property report. 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 listed person or entity property report 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 a suspicious transaction report 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 a suspicious transaction report to FINTRAC if there was an attempted or completed transaction associated with this property.

Reporting entities must submit a listed person or entity property report 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 guidance on submitting reports on listed persons or entities to FINTRAC, see: Reporting listed person or entity property to FINTRAC.

Contact FINTRAC

- **Email**: guidelines-lignesdirectrices@fintrac-canafe.gc.ca (include Special Bulletin FINTRAC-2026-SB002 in the subject line)
- **Telephone**: 1-866-346-8722 (toll free)
- **Mail**: FINTRAC, 24th Floor, 234 Laurier Avenue West, Ottawa ON, K1P 1H7, Canada

Cat. N°. FD4-51/2026E-PDF
ISBN 978-0-660-99492-5

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