INDUSTRY DAY 2026

FINTRAC Webinar

March 25, 2026

Canada

Geneviève Clermont

Assistant Deputy Director, Supervision

Tina Matos

Deputy Director and Chief Compliance Officer, FINTRAC

Private-to-Private Information Sharing

FINTRAC

Policy Overview: Private-to-Private Information Sharing

- Address information silos in private sector
- Align with international standards and best practices as encouraged by the Financial Action Task Force (FATF)
- Strong stakeholder support

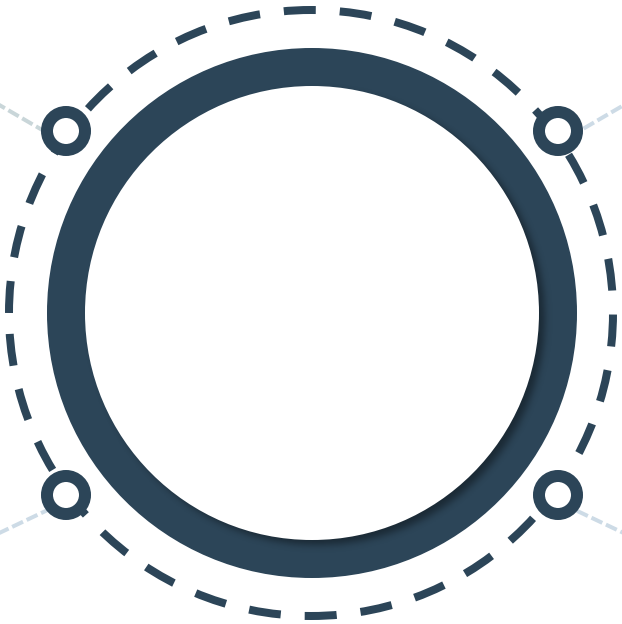
Benefits:

- Enhanced detection of money laundering (ML) and terrorism financing (TF)
- Improve suspicious transaction reporting
- Strong privacy protections – role of the Office of the Privacy Commissioner (OPC)

Guidance Overview: Scope of application

Legal Framework

Purpose



Participants

Conditions

Guidance Overview
Private-to-private information sharing

- ✓ Participation is voluntary
- ✓ Tool to disrupt money laundering and terrorism financing
- ✓ Protection of personal information
- ✓ Strengthens Canada's anti-money laundering and anti-terrorist financing regime

Voluntary nature of participation and its impact on compliance obligations

QUESTIONS

- Are reporting entities required to engage in Private-to-private information sharing?
- Is a reporting entity considered to be in non-compliance when they do not engage in private-to-private information sharing?

Voluntary nature of participation and its impact on compliance obligations

ANSWERS

- The *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* and associated Regulations do not require reporting entities to engage in private-to-private information sharing - It is voluntary.

- In the absence of a private-to-private information sharing, there is no requirement to implement a code of practice.

Roles of FINTRAC and Office of the Privacy Commissioner of Canada

Financial Transactions and Reports Analysis of Canada

- Reviews the code of Practice to ensure compliance with anti-money laundering and anti-terrorist financing obligations under the Act.
- Verifies that the participants are reporting entities.
- Assesses that the code of practice is for the purpose of detecting or deterring money laundering, terrorist activity financing or sanctions evasion.
- Provides comments to the applicant and/or to the OPC within 60 calendar days following the day it is received.

Roles of FINTRAC and Office of the Privacy Commissioner of Canada

Office of the Privacy Commissioner of Canada (OPC)

- Reviews and approves the code of practice when it complies with private-to-private information sharing under section 11.01 of the Act.
- Ensures the Code of Practice complies with the requirements of the Act and provides for substantially the same or greater protection of personal information as that provided under the Personal Information Protection and Electronic Documents Act(PIPEDA).
- Provides a response to the applicant within 120 calendar days (15-day extension if required).
- Determines if revisions to a code of practice are significant within 30 calendar days of submission.

Guidance Overview
Process to submit a code of practice

1. **Establish code of practice**
2. **Submit code of practice to FINTRAC and OPC**
3. **Answer requests for additional information**
4. **OPC informs applicant of decision**
5. **Resubmit at revision or renewal**

How to submit a code of practice

Submit a code of practice

- To submit a code of practice for review and approval to the Office of the Privacy Commissioner of Canada, complete their online information request form, or by phone at 1-800-282-1376.
- To submit a code of practice for review to FINTRAC, email it to codeofpractice-codedepratique@fintrac-canafe.gc.ca.
- Please submit the code of practice to the Office of the Privacy Commissioner of Canada and to FINTRAC on the same day.

Establishing a code of practice with service providers

QUESTION	ANSWER
Can a reporting entity establish a code of practice with a service provider that is not a reporting entity?	Only reporting entities can be participants of a code of practice. However, service providers may support reporting entities to develop a code of practice.

Sharing personal information prior to OPC approval

QUESTION	ANSWER
Can reporting entities that are participants in a code of practice begin to share, collect and use personal information after it has been submitted to FINTRAC and the Office of the Privacy Commissioner of Canada, but before it is approved by the Office of the Privacy Commissioner of Canada?	Before any personal information can be shared between participating reporting entities, the code of practice must be **approved** by the Office of the Privacy Commissioner of Canada.

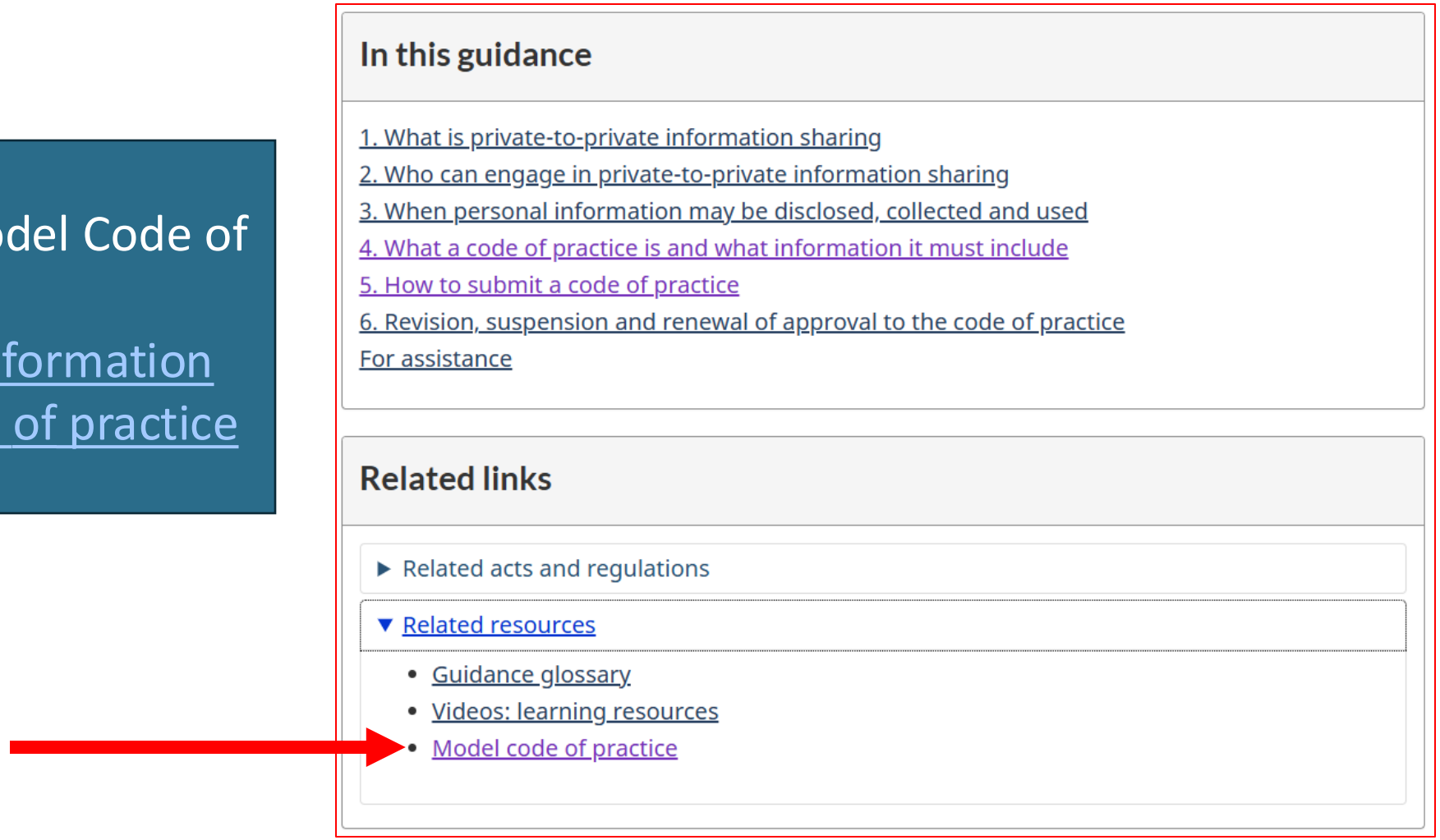
Code of practice renewal period

QUESTION	ANSWER
When a revised code of practice is **approved** by the OPC, when does the five-year period for renewal begin?	The requirement to apply for re-approval after 5 years is based on the most recent approval date, which includes the approval date of the revised code of practice.

Model Code of Practice

Where to find the model Code of practice?

Private-to-private information sharing - Model code of practice



Model Code of Practice - General Disclaimer

DISCLAIMER

- The model Code of practice is meant for general guidance only.
- Each section highlights examples of what could be included in a Code of practice.
- Those who submit should develop and determine the information and details necessary to meet requirements for their particular circumstance.
- Emulating the model Code of practice is not a guarantee of approval by the Office of the Privacy Commissioner.

What is the purpose of the model code?

ANSWER

- Provides an example of a Code of practice for reporting entities to build upon.
- Illustrates elements of Code of practice requirements in the PCMLTFR.
- Demonstrates the implementation of PIPEDA requirements.

Model Code of Practice - Outline of the model Code of practice

As required by s.160 of the PCMLTFR:

1. Application – *Identifies who the code applies to*
2. Purposes for which personal information may be disclosed, collected or used
3. Personal information that may be disclosed, collected or used
4. Manner of sharing of personal information
5. Measures to ensure the protection of personal information disclosed, collected or used
6. Compliance with the requirements of the PCMLTFA
7. Provisions for substantially the same or greater protection of personal information as that provided under PIPEDA

What should be included in a Code of practice?

ANSWER

- Section 4 of FINTRAC's private-to-private information sharing guidance outlines the elements that must be included in a CoP.

- The Code of practice must be sufficiently detailed to demonstrate how each element will be operationalized by the REs involved. The Model Code of practice provides an example of what could be considered in the voluntary development of a Code of practice.

What consists FINTRAC's review of the Code of practice?

ANSWER

FINTRAC's review focuses on whether the proposed code of practice aligns with the objectives of the PCMLTFA. This could include:

- Whether the information sharing practices are clearly designed to detect, deter, and prevent ML, TF or SE.
- Whether the type of personal information to be shared is appropriate, necessary and proportionate to achieving the objectives.
- Whether the code of practice follows the PCMLTFA and the associated Regulations.

Participant acknowledgement

QUESTION	ANSWER
How should applicants document the acknowledgement from each participant confirming their approval of the code of practice and its submission?	FINTRAC's guidance on private-to-private information sharing indicates a Code of practice must include the reporting entity name and reporting entity number of each participating reporting entity for validation purposes. Under subsection 161(2) of the PCMLTFR, each participant must acknowledge approval of the code and consent to its submission to the OPC. This can be done through a brief written statement in an Annex and could include participant signatures.

Can a single party code be submitted?

ANSWER

Under subsection 11.01 (1) of the PCMLTFA, a person or entity referred to in section 5 may disclose an individual's personal information to another person or entity referred to in section 5 without the individual's knowledge or consent. The private-to-private information sharing authority is tied to sharing between two or more reporting entities, and this is what is expected to be included within the code.

Sharing with other REs who have an approved code of practice

QUESTION	QUESTION
Can a reporting entity with an approved Code of practice share with another reporting entity that has an approved code of practice?	No, Code of practice approvals are agreement-specific and not universal. In line with subsection 11.01(1) of the PCMLTFA, information may be shared between two or more reporting entities if all requirements are met, including the requirement to operate under an approved code of practice.

Guidance on Ministerial Directives

FINTRAC

Ministerial Directives

- Under Part 1.1 of the PCMLTFA, **The Minister of Finance** may:
  - Issue directives that require reporting entities to apply countermeasures to transactions coming from or going to designated foreign jurisdictions or entities; and
  - Recommend the introduction of regulations to restrict reporting entities from entering into a financial transaction coming from or going to designated foreign jurisdictions or entities.
- FINTRAC will inform reporting entities that a directive has been issued. Each directive will include an outline of countermeasures that are limited to the same activities for which reporting entities already have obligations. The countermeasures will enhance or add to these obligations.
- Directives will specify the date they come into force and will remain in force until officially revoked, suspended or amended.

What are my obligations as a reporting entity?

- **Monitor notifications** from FINTRAC when a ministerial directive is issued.
- Ministerial directives may require you to **implement enhanced due diligence measures**, these countermeasures add to existing obligations and does not replace them:
  - Enhanced risk assessment and monitoring;
  - Additional know your client and client identification;
  - Tighter record-keeping; and
  - Restrictions or conditions on certain transactions.
- **Implementing internal compliance measures:**
  - Integrate the directive into internal compliance policies and procedures;
  - Update employee training;
  - Adjust systems to detect relevant transactions; and
  - Maintain all associated records (client identification, transaction records involving targeted jurisdictions, etc).

Compliance with Ministerial Directives

- FINTRAC will monitor and assess compliance with directives, in accordance with the PCMLTFA.
- To assess compliance, the PCMLTFA gives FINTRAC the authority to examine the records and inquire into the business and affairs of any entity covered under the Act.
- FINTRAC can issue administrative monetary penalties to address instances of non-compliance and may also disclose cases of non-compliance to law enforcement when there is extensive non-compliance or little expectation of immediate or future compliance.
- The existing administrative monetary penalties regime will be extended to all directives, and failure to comply with a directive could result in a penalty.

Ministerial Directives currently in force: Sanctions Evasion Risks

Updates to the Ministerial Directives on Russia and the Democratic People's Republic of Korea

May 22
2025

Updates to the Ministerial Directive on the Islamic Republic of Iran

November 15
2025

Ministerial Directive on Iran: Expanded Scope & Enhanced Measures

Correspondent Banking Measures:

An entity referred to in subsection 9.4(1) of the Act must:

- Consider the **risk of a sanctions evasion offence** associated with Iran when it enters into a correspondent banking relationship and when conducting ongoing monitoring of that correspondent banking relationship.

- **Assess measures** taken by jurisdictions, where the foreign financial institution was incorporated and in which it conducts transactions, to implement the United Nations Security Council sanctions against Iran.

Ministerial Directive on Iran: Reporting instructions

All reporting entities must report any transaction originating from or bound for Iran to FINTRAC by:

- Using the **corresponding threshold report** (Large Cash Transaction Report, Large Virtual Currency Transaction Report, Electronic Funds Transfer Report) even when the transaction is under $10,000
    - 24-hour rule applies.
- Using **suspicious transaction reports** when reporting obligations extend to activities that previously had no reporting requirement. For example:
    - Domestic electronic funds transfers.
    - Real estate brokerages sending or receiving international electronic funds transfers originating from or bound for Iran.
    - Title insurers receiving cash or virtual currency originating from or bound for Iran.
- **Interim measure for Casinos:**
    - With current reporting mechanisms, casinos are instructed to use suspicious transaction reports to report under-threshold casino disbursements originating from or bound for Iran.

Countering Extortion Partnership

FINTRAC

Announcing the Countering Extortion Partnership

'Enough is enough': Canadian intelligence experts to focus on extortion crime, federal minister says

On February 19, Minister Champagne announced new measures to strengthen Canada's ability to detect, disrupt, and prevent extortion across Canada, especially in the most affected areas like Ontario, British Columbia, and Alberta.

The Minister highlighted the objectives of improving how financial intelligence is collected and shared so that law enforcement will be better equipped to trace criminal networks, support investigations, and hold those responsible accountable.

Countering Extortion Partnership and Operation TAPEX

As part of the **Countering Extortion Partnership** initiative, FINTRAC has launched Operation TAPEX (Timely Analysis of Proceeds from Extortion) to support analysis related to proceeds generated by criminals extorting communities and individuals.

The overall Countering Extortion Partnership will see a number of collaborative actions :

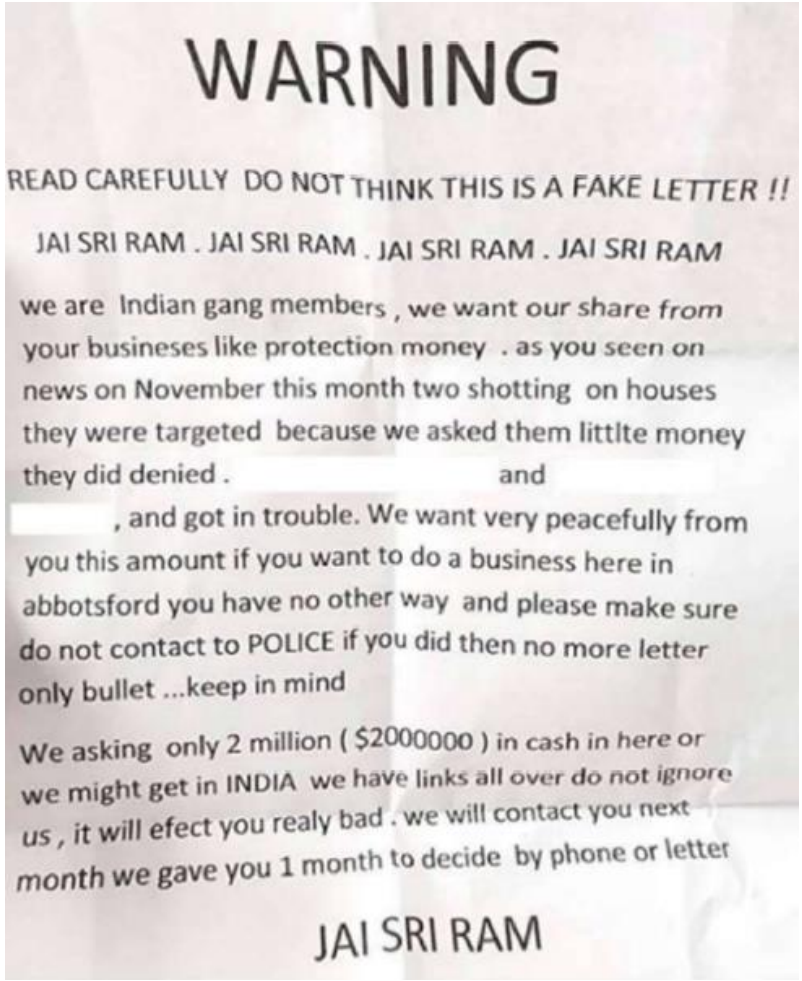
- Consultation and collaboration with entities most at risk, to identify and coordinate on key indicators through a **Targeted Indicator Profile** (TIP).
- **Work with police of jurisdiction** to ensure their expertise and on-the-ground knowledge informs advice and guidance.
- **Information sessions** for most implicated sectors, to provide information on trends, methods and indicators.
- **Publication of a special bulletin** that communicates to the wider reporting entity community strategic intelligence on money laundering activities related to extortion and building on these outreach activities.

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;
- third parties (e.g., virtual asset service providers) exchanging fiat currency for cryptocurrency; and,
- relevant customer and counterparty cryptocurrency wallet addresses, where available.

Financial Intelligence context

- Extortion schemes targeting South Asian communities are profit-driven, with perpetrators exploiting community networks for financial gain.
  - reported across Canada, with media attention more pronounced in ON, BC, and AB.
- *Multiple* criminal elements are suspected of involvement, including BISHNOI GANG, BAMBIHA GANG, and "copycats".
  - Experienced in drug trafficking, human smuggling and insurance fraud schemes.
- Victims—often small and midsize business owners—describe anonymous calls or messages demanding large payments.
  - Immediate demands for lump sum payments, rapid fund transfers, or cash deliveries arranged under duress.
  - Victims probably negotiate the amounts to be paid.
- Extortionists abuse financial institutions (banks), money services businesses (MSBs), and credit unions.
  - Substantial in-bank and ATM cash placement, heavy EMT layering and flow-through.
  - Credible indications that international remittance companies and cryptocurrency exchanges play a role.



WARNING

READ CAREFULLY DO NOT THINK THIS IS A FAKE LETTER !!

JAI SRI RAM . JAI SRI RAM . JAI SRI RAM . JAI SRI RAM

we are Indian gang members , we want our share from your busineses like protection money . as you seen on news on November this month two shotting on houses they were targeted because we asked them littIte money they did denied . and , and got in trouble. We want very peacefully from you this amount if you want to do a business here in abbotsford you have no other way and please make sure do not contact to POLICE if you did then no more letter only bullet ...keep in mind

We asking only 2 million ($2000000) in cash in here or we might get in INDIA we have links all over do not ignore us , it will efect you realy bad . we will contact you next month we gave you 1 month to decide by phone or letter

JAI SRI RAM

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.

- Student profile inconsistent with activity: A young South Asian man claiming to be an international student shows payments to schools and immigration services, but his deposits suggest unrelated work (e.g., trucking, music, construction) and he may use aliases or stage names.
- Unexplained and structured cash deposits: He makes unusual cash deposits—sometimes structured—across multiple branches and ATMs, then quickly sends the funds via email money transfers to unknown recipients.
- High-volume email money transfers: He sends and receives an unusually large number of email money transfers inconsistent with student income, sometimes showing funnelling patterns or flow-through transactions.

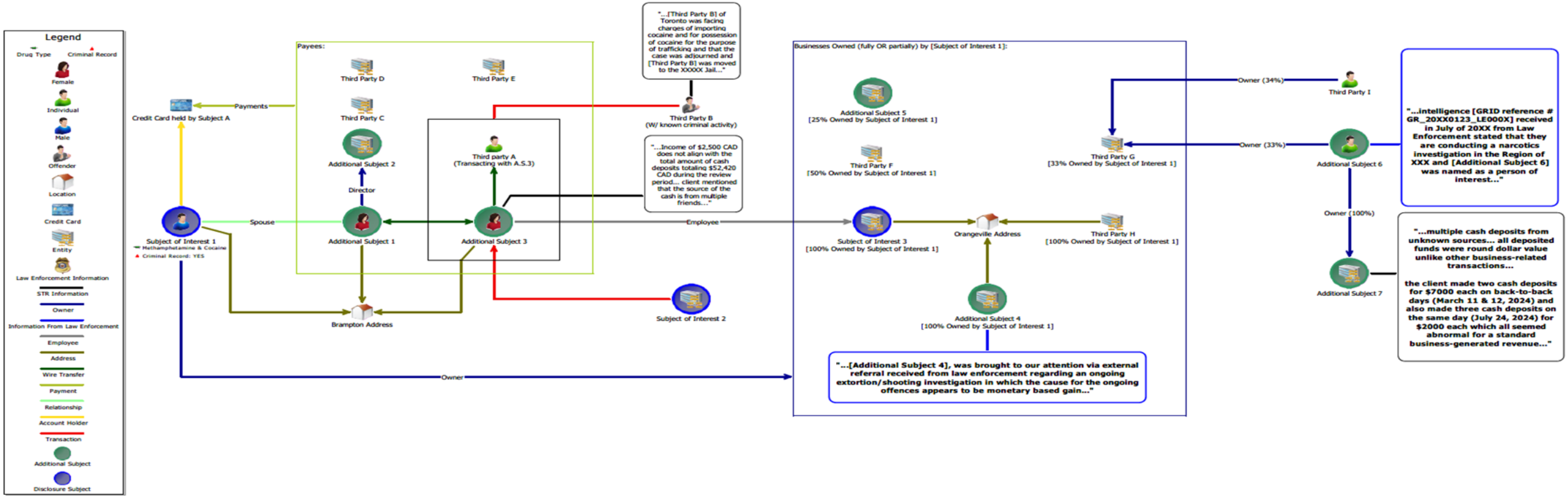
Indicators (Cont'd)

- Adverse media links: His name may appear in media connected to extortion, violence, or other crimes in South Asian communities. Lack of media does not negate suspicion when other indicators exist.
- Abnormal remittances from India: He receives unusually large or frequent transfers from India described as family support or property-related, sometimes structured below thresholds or split across joint accounts.
- Victim behaviour: Likely to be a local business owner that appears distressed or nervous, attempting large cash withdrawal or wire transfer inconsistent with past transaction behaviours.
  - May be receiving direction or coaching as they attempt to liquidate long-term investments or execute large or multiple outgoing wires to new counterparties.
  - Victims may also raise money laundering suspicions.
- Illicit narcotics trade: May display financial indicators associated with Project Legion (illicit cannabis), to include receiving payments from individuals with contact names associated with illicit drugs.

Case Example

FINTRAC CANAFE

Chart: Sanitized overview of transactions/relationships identified in Financial Transaction Reports



STRs: Reporting Fraud and Best Practices

FINTRAC

Fraud Prevention Month

- Fraud is one of the fastest-growing crimes in Canada, but it often goes unnoticed and unreported - hidden behind convincing technology or in everyday online interactions or crossing international borders.
- Data from the Canadian Anti-Fraud Centre (CAFC) shows that Canadians lost over **$704 million** to fraud in 2025, with reported losses since 2022 now surpassing **$2.4 billion**. These losses represent only a fraction of the harm, because **only 5% to 10% of frauds are reported**.

Quick facts

In 2025, the top three most reported types of fraud were identity fraud, investment fraud, and service fraud – all designed to get you to pay or give away sensitive information like your social insurance number, passwords or banking details. The top three frauds reported with the highest financial impacts were investment fraud, romance fraud, and job fraud.

The National Risk Assessment (NRA)

The 2025 Assessment of Money Laundering and Terrorist Financing Risks in Canada, also referred to as the "National Risk Assessment," represents the Government of Canada's understanding of money laundering and terrorist financing risks at the national level.

The AML/ATF Regime operates on three interdependent pillars:

(i) policy and coordination;

(ii) prevention and detection; and

(iii) investigation, prosecution, and disruption.

Observed supervisory fraud trends

FINTRAC has identified a high volume of unreported STRs in recent supervisory activities across all sectors related to fraud.

Reporting entities are uncertain if all fraud scenarios are reportable to FINTRAC within an STR to comply with the PCMLTFA/PCMLTFR, such as victims of fraud.

Threshold for Suspicion

Simple Suspicion

- **Hunch or intuition** leads you to think that an ML or TF offence may be occurring
- Cannot articulate reasons for suspicion

Reasonable Grounds to Suspect

- Submit an STR to FINTRAC
- Based on an assessment of facts, context and indicators there is a **possibility** that an ML or TF offence is occurring
- Able to present reasons why it is suspicious but they do not need to be proven or verified

Reasonable Grounds to Believe

- There is a **probability** that an ML, TF or SE offence is occurring
- Ability to present a set of verified facts can be proven and support this suspicion

Definition of a Money Laundering Offence

A money laundering offence involves various acts committed with the intention to conceal or convert property or the proceeds of property (such as money) knowing or believing that these were derived from the commission of a designated offence.

In this context, a designated offence means most serious offences under the Criminal Code or any other federal Act. It includes, but is not limited to, those relating to illegal drug trafficking, bribery, **fraud**, forgery, murder, robbery, counterfeit money, stock manipulation, tax evasion, and copyright infringement.

STR Requirements & Best Practices

Regulatory Requirements

- Include all suspicious transactions **in the correct form and manner.**
- Provide **all available** KYC data
- Clearly articulate **why** the STR is being filed (i.e. what led you to conclude that RGS was met)

Strong STRs include…

- **Consistent** formatting and description
- **Stand-alone narratives** for multiple related STRs, instead of only noting "see STR #123".
- A clear indication of **how** the suspicious activity was identified
- All **relevant behavioral/contextual indicators** that form part of your suspicion

STRs: Four Basic Rules for REs

Must include **transaction(s)/ attempted transaction(s)**

Must have "**reasonable grounds to suspect ML/TF**"

Must send STR/STRs "**as soon as practicable**"

Details, details, details…**And more details**!

Policy Interpretation 10876

Question: Is a suspicious transaction report (STR) required to be filed If you determine, or suspect, that a client is a victim of fraud, whether the transaction is completed or not?

Answer: Yes, pursuant to section 7 of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA), every person or entity referred to in section 5 shall, in accordance with the regulations, report to the Centre every financial transaction that occurs or that is attempted in the course of their activities and in respect of which there are reasonable grounds to suspect: 1. the transaction is related to the commission or the attempted commission of a money laundering (ML) offence; 2. the transaction is related to the commission or the attempted commission of a terrorist activity financing (TF) offence.

FINTRAC does not limit the types of fraud that REs can report on. Therefore, it is inclusive of many mediums that allow for the misappropriation of financial assets through fraud, including the types of fraud you have mentioned. All business services of an RE that allow for the possibility of fraud through any medium (e.g., credit cards) should be taken into consideration against the obligation to submit an STR.

Policy Interpretation 12654C

Question: Does FINTRAC have parameters around what type would constitute confirmed fraud? For example: Cheque Fraud, Internet Fraud, Wire Fraud etc.

Answer: FINTRAC does not limit the types of fraud that REs can report on. All business services of an RE that allow for the possibility of fraud through any medium should be taken into consideration against the obligation to submit an STR.

ML/TF Indicators - Fraud Publications

- Operational alert: Laundering of the proceeds of romance fraud
- Operational alert: Laundering the proceeds of tax evasion in real estate
- Operational brief: Indicators of money laundering in financial transactions related to real estate
- Special Bulletin on COVID-19: Trends in Money Laundering and Fraud
- Money laundering and terrorist financing indicators—Financial entities
- Updated indicators: Laundering the proceeds of crime through underground banking schemes
- FINTRAC publishes indicators on the laundering of proceeds from illicit cannabis in support of Project Legion

Importance of Reporting Fraud-Related STRs

Project Chameleon Impact:

- Since 2017, increased STRs involving fraud victims have enhanced FINTRAC's intelligence capabilities.
- Victim information helps FINTRAC identify complex fraud schemes and interconnected cases.
- Enables law enforcement notifications to victims, helping to disrupt fraudulent activity.

***Project Fletcher*:** Eight individuals arrested and five others wanted in a long-running $3M fraud case in Durham Region.

- The forensic audit uncovered 270 fraudulent cheques tied to 8 subcontractor companies and 22 bank accounts.
- The investigation revealed extensive money-laundering activity involving cheque-cashing **businesses, multiple financial institutions, and movement of funds** across Durham Region, the GTA, and internationally.

Frequently Asked Questions - Fraud

How does filing on victims of fraud help FINTRAC, don't we have to consider privacy legislation on only reporting on criminals/suspects in our STRs?

Do we have to file an STR in instances when we only see the placement stage and no actual movement of funds occurred in fraud related scenarios?

Do we have to file an STR to FINTRAC when no confirmed perpetrator is identified ?

Resources Related to Fraud and STR Reporting

- **Guidance**
- **STR videos**
  - Video 1 – The importance of suspicious transaction reports
  - Video 2 – Understanding reasonable grounds to suspect
  - Video 3 – What to consider when submitting a suspicious transaction report
- **Canadian Anti-Fraud Centre**

Closing Remarks

FINTRAC

Thank You!

@FINTRAC_Canada

Join FINTRAC's mailing list

guidelines-lignesdirectrices@fintrac-canafe.gc.ca

End of Session

@FINTRAC_Canada

Join FINTRAC's mailing list

guidelines-lignesdirectrices@fintrac-canafe.gc.ca