# Intro to Canadian Anti Money Laundering

## 1. The Legislative and Regulatory Ecosystem

The foundation of AML compliance in Canada is built upon a specific set of federal statutes. Unlike jurisdictions with a single, monolithic regulator, Canada employs a multi-agency approach.

### 1.1 The Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)

The *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA) is the primary legislative vehicle for AML in Canada. Originally enacted in 2000 as the *Proceeds of Crime (Money Laundering) Act*, it was fundamentally amended in December 2001 following the 9/11 terrorist attacks to include the financing of terrorism, adopting its current name. The Act applies to a wide range of "Reporting Entities" (REs), which includes banks, credit unions, life insurance companies, securities dealers, casinos, and money services businesses (MSBs).2

The PCMLTFA serves three primary functions:

1. **Establishment of FINTRAC:** It created the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) as an independent agency with a mandate to receive financial reports, analyze them, and disclose "financial intelligence" to law enforcement and intelligence agencies when specific thresholds are met.3
2. **Obligations:** It sets out the core duties of REs, including customer identification (Know Your Client or KYC), record keeping, transaction reporting, and the mandatory implementation of a compliance program.1
3. **Enforcement:** It provides the mechanism for Administrative Monetary Penalties (AMPs) for non-compliance, as well as criminal offenses for egregious failures to report or retain records.3

### 1.2 The Criminal Code of Canada

While the PCMLTFA dictates the *regulatory* responsibilities of a bank (e.g., filing reports), the *Criminal Code* defines the *offense* of money laundering itself. This distinction is vital. A bank does not determine guilt; it identifies suspicion. However, that suspicion is predicated on the definition of the crime found in the Code.

Under **Section 462.31** of the *Criminal Code*, a money laundering offense involves any act committed with the intention to conceal or convert property or the proceeds of property, knowing or believing that these were derived from the commission of a "designated offense".2

* **Designated Offenses:** This category is broad, encompassing most serious crimes such as illegal drug trafficking, bribery, fraud, forgery, robbery, counterfeit money operations, stock manipulation, and tax evasion.
* **Extraterritoriality:** Crucially for international banks, the offense extends to property or proceeds derived from illegal activities that took place *outside* Canada, provided the act would have been a crime if it had occurred within Canada. This means a Canadian bank can be liable for handling funds generated by a crime in a foreign jurisdiction.2

In the Canadian Criminal Code, the definitions for terrorist activity and the financing of terrorism are primarily found in **Section 83.01**. These definitions serve as the foundation for all terrorism-related offences in Canada.

* **Terrorist Activity**: The Code uses a two-part definition to cover both specific international agreements and a general "catch-all" description:
* **Part A (Specific Acts):** Any act or omission that constitutes an offence under specific international counter-terrorism conventions (e.g., aircraft hijacking, attacks on internationally protected persons, or nuclear terrorism).
* **Part B (The General Definition):** This covers any act or omission (inside or outside Canada) that meets the following three criteria:
  1. **Objective:** It is committed in whole or in part for a **political, religious, or ideological** purpose, objective, or cause.
  2. **Intention:** It is intended to **intimidate the public** (regarding its security) or **compel a government** or organization to do (or refrain from doing) something.
  3. **Harm:** It intentionally causes specific severe consequences, such as:
     + Death or serious bodily harm.
     + Endangering a person’s life.
     + Serious risk to public health or safety.
     + Substantial property damage likely to result in the harms above.
     + Serious disruption of an essential service, facility, or system (not including lawful protest or strikes).

### 

### 

### Financing of Terrorism

Terrorist financing is defined through several specific offences in **Sections 83.02 to 83.04**. These laws target the movement of money or property before a terrorist act even occurs.

| **Offence Section** | **Description** |
| --- | --- |
| **Section 83.02** | **Providing or collecting property** intending or knowing it will be used to carry out a terrorist activity. |
| **Section 83.03** | **Providing property or services** for terrorist purposes or for the benefit of a terrorist group. |
| **Section 83.04** | **Using or possessing property** for the purpose of facilitating or carrying out a terrorist activity. |

**Key Legal Distinctions:**

* **Knowledge:** You can be charged even if you don't know the *specific* terrorist act the money will fund; knowing it is for a "terrorist activity" or "terrorist group" is enough.
* **Legitimacy of Funds:** Unlike money laundering (where the money usually comes from a crime), terrorist financing often involves **legitimate funds** (like donations or personal income) that are then used for an illegal purpose.
* **Freeze and Report:** Section 83.08 requires financial institutions to immediately freeze any property they know is owned or controlled by a "listed" terrorist entity.

### 1.3 The Regulatory Landscape: FINTRAC and OSFI

Canada operates under a "dual-regulator" model for financial institutions, although recent years have seen a consolidation of AML supervision responsibilities.

#### FINTRAC: The Intelligence Unit and AML Supervisor

FINTRAC is the primary regulator for the PCMLTFA. It operates at arm's length from law enforcement, ensuring that the privacy of Canadian financial data is protected until a threshold of suspicion is met. Its mandate is twofold:

1. **Intelligence:** To analyze the millions of reports submitted by REs (Suspicious Transaction Reports, Large Cash Transaction Reports, etc.) and disclose tactical intelligence to police and national security agencies.1
2. **Compliance:** To ensure REs are meeting their obligations. FINTRAC conducts examinations of banks to test their policies, training, and reporting systems. It has the power to levy significant fines (AMPs) for non-compliance.3

#### OSFI: The Prudential Regulator

The Office of the Superintendent of Financial Institutions (OSFI) is responsible for the safety and soundness of federally regulated financial institutions (FRFIs). Historically, OSFI maintained its own AML guideline, **Guideline B-8 (Deterring and Detecting Money Laundering and Terrorist Financing)**. However, in a strategic shift to eliminate duplication and regulatory burden, OSFI **rescinded Guideline B-8** effective July 26, 2021.7

This rescission signaled a transfer of the primary AML *supervisory* mandate to FINTRAC. However, OSFI remains deeply involved from a *prudential* perspective.

* **Guideline E-13 (Regulatory Compliance Management):** OSFI now oversees AML risk through the lens of Guideline E-13. It expects banks to manage AML/ATF risk as they would any other regulatory risk that could threaten the bank's solvency or reputation.8
* **Material Risk:** OSFI focuses on "material risk." If a bank's AML controls are so deficient that they invite massive fines or catastrophic reputational damage (thereby threatening the bank's stability), OSFI will intervene.
* **Information Sharing:** Under the PCMLTFA, FINTRAC and OSFI are authorized to share information. If FINTRAC identifies systemic failures in a bank's AML program during an exam, they can disclose this to OSFI, who may view it as a failure of corporate governance.9

### Table 1: Regulatory Division of Labour

| **Feature** | **FINTRAC (The AML Supervisor)** | **OSFI (The Prudential Regulator)** |
| --- | --- | --- |
| **Primary Mandate** | Detection/Prevention of ML/TF; Financial Intelligence. | Prudential Safety & Soundness; Stability of Financial System. |
| **Key Legislation** | *PCMLTFA* & Regulations. | *Bank Act*, *OSFI Act*. |
| **AML Role** | Direct assessment of compliance with PCMLTFA; Issuing AMPs. | Assessing broad risk management (Guideline E-13); ensuring solvency. |
| **Output** | Intelligence disclosures to law enforcement. | Intervention/Supervision of bank capital & governance. |
| **Current Status** | Primary AML auditor and enforcer. | Rescinded specific AML guideline (B-8); relies on general risk guidelines. |

## 2. The Compliance Program: The "Six Elements"

Historically, the industry referred to the "Five Pillars" of an AML program. However, recent amendments and FINTRAC guidance have refined this into **six mandatory elements** that must be implemented by all reporting entities. For a major bank, these are not abstract concepts but distinct operational departments.11

### 2.1 Element 1: The Compliance Officer (CAMLO)

The Act requires the appointment of a person responsible for the implementation of the program. In a D-SIB, this role is the **Chief Anti-Money Laundering Officer (CAMLO)**.

* **Authority & Independence:** The CAMLO must have the necessary authority and access to resources to implement the program effectively. Crucially, for a large business, the CAMLO should have **independent oversight**, meaning they are not directly involved in the receipt, transfer, or payment of funds (revenue generation). They must have direct access to the Board of Directors to report on risks without filtering by business line management.11
* **Knowledge Requirement:** The CAMLO must have detailed knowledge of the business's functions and structure, as well as the sector's specific ML/TF risks. This includes understanding typologies (methods used by criminals) relevant to banking, such as trade-based money laundering or smurfing.11

### 2.2 Element 2: Policies and Procedures

Banks must develop and apply written compliance policies and procedures. These must be kept up to date and, in the case of an entity, approved by a senior officer.11

* **Comprehensive Scope:** These policies must cover every regulatory obligation: how to verify ID, how to determine a PEP, how to report an STR, and how to keep records.
* **Operational Reality:** In a Big 5 bank, this "element" manifests as a vast library of Standard Operating Procedures (SOPs) and Enterprise Policies. These documents translate the vague legal requirement of "take reasonable measures" into specific keystrokes for a teller or back-office analyst.12

### 2.3 Element 3: Risk Assessment

The bank must conduct and document a risk assessment of its business. This is the cornerstone of the **Risk-Based Approach (RBA)**. The assessment must consider specific factors mandated by FINTRAC 13:

1. **Clients and Business Relationships:** Assessing the risk of the customer base (e.g., cash-intensive businesses, non-residents, PEPs).
2. **Products, Services, and Delivery Channels:** evaluating the inherent risk of offerings (e.g., wire transfers and private banking are higher risk than retail savings accounts; non-face-to-face account opening is higher risk than in-branch).
3. **Geography:** Assessing risks related to countries where the bank operates or where clients transact (e.g., jurisdictions subject to sanctions or with weak AML regimes).
4. **New Technologies:** Assessing the impact of new tech on ML risks (e.g., introducing cryptocurrency custody services or AI-driven lending).
5. **Other Relevant Factors:** Any other factor specific to the bank, such as turnover or structural complexity.11

### Inherent Risk (The "Raw" Risk)

Inherent risk is the level of risk that exists **before** you apply any controls or mitigation measures. It is the "gross risk" or the baseline threat posed by your business operations.

* **How it’s identified:** You look at the "raw" factors of your business that could be exploited for money laundering or terrorist financing.
* **Key Categories (FINTRAC pillars):**
  + **Products & Services:** Do you offer anonymous prepaid cards or high-value wire transfers?
  + **Delivery Channels:** Do you onboard clients face-to-face, or is it all online (higher risk)?
  + **Geographic Risk:** Are you doing business in jurisdictions with high crime rates or weak AML laws?
  + **Client Risk:** Are you dealing with Politically Exposed Persons (PEPs) or complex corporate structures?

### Residual Risk (The "Leftover" Risk)

Residual risk is the level of risk that remains **after** you have implemented your AML controls and determined their effectiveness. It is the "net risk."

* **The Calculation:** Inherent Risk - Control Effectiveness = Residual Risk
* **How it’s managed:** Once you know the residual risk, your leadership team must decide if it falls within the company’s **Risk Appetite**.
* **Outcomes:** If the residual risk is too high, you have three choices:
  1. **Enhance Controls:** Add more monitoring or stricter ID verification.
  2. **Avoid the Risk:** Stop offering that product or exit that client relationship.
  3. **Accept the Risk:** Acknowledge it is there but decide it is manageable (and document why).

### Comparison Table

| **Feature** | **Inherent Risk** | **Residual Risk** |
| --- | --- | --- |
| **Status** | Before controls (Gross) | After controls (Net) |
| **Focus** | Vulnerabilities and threats | Control gaps and remaining exposure |
| **Goal** | To understand what *could* happen | To understand what is *likely* to happen now |
| **Regulatory View** | FINTRAC expects you to document this first | FINTRAC uses this to judge if your program is working |

### 2.4 Element 4: Training Program

A written, ongoing compliance training program is mandatory for employees, agents, or mandataries who deal with customers or transactions.

* **Content:** The training must cover ML/TF concepts, the specific reporting requirements, and the bank's internal policies.
* **Targeted Delivery:** Training must be tailored to the role. A front-line teller needs training on spotting physical cash structuring (smurfing), while a commercial lender needs training on complex corporate structures and trade-based laundering. A compliance analyst needs technical training on filing reports.15

### 2.5 Element 5: Training Plan

Distinct from the training content itself, the regulations require a documented **plan** for delivering and maintaining the training. This element ensures training is not ad-hoc but systematic. The plan must track who was trained, when, and ensure that training is refreshed regularly to capture regulatory changes (e.g., the 2024/2025 amendments).11

### 2.6 Element 6: Effectiveness Review (Two-Year Review)

At least every two years, the compliance program (policies, risk assessment, training) must be reviewed for effectiveness.

* **Auditor Requirements:** The review must be conducted by an internal or external auditor. For a Big 5 bank, this is typically executed by the **Internal Audit** department, which is independent of the Compliance function. The reviewer must be knowledgeable about the Act but not directly involved in the program's operation.11
* **Testing vs. Reviewing:** The review must do more than check if policies exist; it must test if they are working. This involves sampling transaction files to ensure KYC was actually collected, sampling STRs to ensure they were filed on time, and interviewing staff to verify knowledge retention.17 The results must be reported to a senior officer within 30 days.17

## 3. Know Your Client (KYC) and Identity Verification

For a bank, KYC is the primary preventative control. It involves ascertaining the identity of the customer and understanding the nature of their business to establish a baseline for monitoring. FINTRAC prescribes rigid methods for how identity must be verified.

### 3.1 Identification Methods for Individuals

When opening an account, issuing a credit card, or conducting large transactions, a bank must verify the identity of an individual. The "Big 5" rely on specific FINTRAC-approved methods 18:

1. **Government-Issued Photo ID Method:** The most common method. The bank must view a valid, authentic, current government-issued document (federal, provincial, or territorial). It must include a photo and a unique identifying number. Examples include a Driver's License or Passport.
   * *Virtual Verification:* With the rise of digital banking, this can be done remotely if the technology determines the document's authenticity (e.g., using Docusign ID Verification or similar tech that analyzes the ID image).20
2. **Credit File Method:** The bank can refer to a credit file located in Canada that has been in existence for at least three years. The name, address, and date of birth in the file must match the information provided by the client.21
3. **Dual Process Method:** This involves verifying information from **two** reliable sources. The bank must verify either:
   * Name and Address (Source 1) + Name and Date of Birth (Source 2).
   * Name and Address (Source 1) + Name and Financial Account Number (Source 2).
   * Name and Date of Birth (Source 1) + Name and Financial Account Number (Source 2).
   * *Note:* The information must come from reliable sources (e.g., a utility bill, a bank statement from another institution, a CRA notice).18
4. **Affiliate Method:** A bank can rely on the identification previously performed by an affiliate (e.g., the securities arm of the same financial group), provided the affiliate is also a reporting entity.18

### 3.2 Beneficial Ownership (The New Frontier)

One of the most significant shifts in the Canadian regime is the increased focus on **Beneficial Ownership (BO)**. Criminals often use complex corporate structures to hide their involvement. Banks are now required to "pierce the corporate veil."

* **The Requirement:** When opening an account for an entity (corporation, trust, partnership), the bank must obtain the name and address of all beneficial owners.
* **The Threshold:** A beneficial owner is any individual who, directly or indirectly, owns or controls **25% or more** of the entity.22
* **Operational Burden:** Banks must obtain an organizational chart, director names, and ownership breakdown. If the entity is a trust, the bank must identify all trustees, beneficiaries, and settlors.23

**The 2025 Discrepancy Reporting Rule:**

A major operational change comes into force on October 1, 2025. Reporting entities (banks) will be required to verify beneficial ownership information against the Corporations Canada database for federally incorporated companies.

* **Material Discrepancy:** If the information the bank collects (from the client) differs from the information in the government registry, and the discrepancy is "material" (meaningful inconsistency regarding names or ownership), the bank must take action.
* **Mandatory Reporting:** If the bank assesses the client as "high risk" for ML/TF, it **must report the discrepancy** to Corporations Canada within 30 days.23
* **Provincial Registries:** While the federal requirement focuses on the Canada Business Corporations Act (CBCA) registry, banks also interact with provincial registries (e.g., British Columbia's Land Owner Transparency Act registry) to verify ownership for provincial entities. The landscape is fragmented, but the move toward a public, searchable registry is a federal priority.26

### 3.3 Politically Exposed Persons (PEPs) and HIOs

Banks must determine if a client is a Politically Exposed Person (PEP) or a Head of an International Organization (HIO). These individuals pose a higher risk for corruption and bribery.

* **Foreign PEP:** A person who holds or *has held* a prominent public function in a foreign country (e.g., Head of State, Judge, Military General). **Once a Foreign PEP, always a Foreign PEP.** There is no expiration date on this status.28
* **Domestic PEP:** A person who holds or has held a prominent public function in Canada (e.g., Member of Parliament, Mayor, Senator, Judge). A person ceases to be a domestic PEP **5 years** after they leave office.28
* **HIO (Head of International Organization):** The primary person who leads an international organization (e.g., UN, NATO, OECD). They cease to be an HIO **5 years** after leaving the post.28
* **Family Members and Close Associates:** The risk extends to family (spouse, child, parent, sibling) and close associates (business partners, romantic partners).
  + *Rule:* If the primary PEP loses their status (e.g., a domestic PEP 5 years after leaving office), the family members also lose their status. However, close associates remain designated until the *relationship* ends.28

**Operational Impact:** High-risk PEPs/HIOs require **Enhanced Due Diligence (EDD)**. This includes establishing the **Source of Wealth (SoW)** (how they acquired their accumulated net worth) and **Source of Funds (SoF)** (the origin of the specific funds in the transaction). Senior management approval is often required to keep these accounts open.31

## 4. Transaction Reporting: The Data Pipeline

The "Big 5" banks are essentially data factories for FINTRAC. They submit millions of reports annually. Understanding the specific triggers, timelines, and aggregation rules for these reports is non-negotiable, as automated failures here lead to massive Administrative Monetary Penalties.

### 4.1 Suspicious Transaction Reports (STRs)

The STR is the most qualitative report. Unlike others based on objective thresholds, this relies on the judgment of the bank.

* **Trigger:** The bank must report if there are "reasonable grounds to **suspect**" that a transaction (completed or attempted) is related to the commission of a money laundering or terrorist financing offense.
* **Threshold:** There is no monetary minimum. A $5 transaction can be suspicious.
* **Timeline:** The report must be submitted "as soon as practicable" after the suspicion is established. This implies a reasonable time for analysis but penalizes undue delay.
* **Attempted Transactions:** If a client attempts a transaction (e.g., asks to deposit cash but walks away when asked for ID), this **must** be reported as an Attempted Suspicious Transaction.33

### 4.2 Large Cash Transaction Reports (LCTRs)

* **Trigger:** The receipt of **$10,000 or more in cash** (physical currency—coins and notes) in a single transaction.
* **The 24-Hour Rule (The Aggregator):** This is a complex logic rule. A bank must aggregate multiple cash transactions under $10,000 if:
  1. They total $10,000 or more within a **consecutive 24-hour window**.
  2. The bank knows they are conducted by the **same person/entity** OR on behalf of the **same person/entity** OR for the **same beneficiary**.
* **Timeline:** The LCTR must be submitted within **15 calendar days** of the transaction.5
* **Operational Challenge:** Implementing the 24-hour rule requires sophisticated systems that link transactions across different branches and channels (e.g., ATM deposits vs. Teller deposits) in real-time.

### 4.3 Electronic Funds Transfer Reports (EFTRs)

* **Trigger:** The sending or receiving of an **international** electronic funds transfer (EFT) of **$10,000 or more**.
  + *Note:* Domestic wires (within Canada) are not reportable to FINTRAC under this specific rule (though they are subject to the Travel Rule).
* **Timeline:** Within **5 working days** of the transmission.36
* **Scope:** This typically involves SWIFT MT103 messages. The bank must report both:
  + **Outgoing:** When the bank initiates the transfer (Client sends money abroad).
  + **Incoming:** When the bank is the final recipient (Client receives money from abroad).37
  + *Intermediaries:* If the bank is merely an intermediary (passing funds between two other banks), it does not file the EFTR, but must pass on the Travel Rule data.

### 4.4 Large Virtual Currency Transaction Reports (LVCTR)

* **Trigger:** The receipt of virtual currency (VC) equivalent to **$10,000 or more**.
* **24-Hour Rule:** The same aggregation logic applies here as with cash.35
* **Relevance:** While major Canadian banks have historically been risk-averse regarding direct crypto custody, they act as banking partners for crypto exchanges (MSBs). If the bank were to launch a crypto custody product, this reporting stream would become active.33

### 4.5 Terrorist Property Reports (TPR)

* **Trigger:** If a bank knows that property in its possession or control is owned or controlled by or on behalf of a terrorist or terrorist group.
* **Action:** The bank must freeze the property immediately and report it to FINTRAC and the RCMP **without delay** (effectively immediately). This is a rare but critical report.39

### Table 2: Summary of FINTRAC Reporting Requirements

| **Report Type** | **Trigger Threshold** | **Timeline** | **Key Operational Nuance** |
| --- | --- | --- | --- |
| **STR** | No minimum; Subjective suspicion. | As soon as practicable. | Includes *attempted* transactions. Requires narrative explanation. |
| **LCTR** | $10,000+ Physical Cash. | 15 Calendar Days. | 24-Hour Rule applies. Aggregates deposits across branches. |
| **EFTR** | $10,000+ International Wire. | 5 Working Days. | Includes SWIFT MT103. Separate logic for Incoming vs. Outgoing. |
| **LVCTR** | $10,000+ Virtual Currency. | 5 Working Days. | 24-Hour Rule applies. Applies to "receipt" of VC. |
| **TPR** | Any value (Terrorist Property). | Without Delay (Immediate). | Requires immediate asset freeze. |

## 5. Sanctions and Ministerial Directives

The bank must screen its entire client base and all cross-border payments against various lists to ensure it is not facilitating business for designated states or individuals.

### 5.1 The Lists and Legislation

Banks screen against the **Consolidated Canadian Autonomous Sanctions List** and the **OSFI Designated Persons List**. These lists are derived from three key acts:

1. **United Nations Act (UNA):** Implements UN Security Council resolutions. These are mandatory global sanctions.
2. **Special Economic Measures Act (SEMA):** Allows Canada to impose sanctions (unilaterally or with allies) in response to grave breaches of international peace. This acts as the legal basis for sanctions against Russia, Iran, and North Korea.40
   * *Technical Assistance:* SEMA sanctions often include bans on providing "technical assistance" (data, blueprints, software) to designated states, which banks must monitor in trade finance transactions.42
3. **Justice for Victims of Corrupt Foreign Officials Act (JVCFOA):** Known as the "Magnitsky Law," this targets foreign nationals responsible for gross human rights violations. It allows for asset freezes and dealings bans on individuals regardless of their country's official sanction status.41

**Frequency:** OSFI expects screening to happen **"without delay."** For a D-SIB, this translates to **daily** batch screening of the client database and **real-time** screening of wire transfers (halting the wire before it leaves the bank).43

### 5.2 Ministerial Directives

The Minister of Finance has the authority under the PCMLTFA to issue directives that require banks to take specific countermeasures against high-risk jurisdictions.

* **Current Targets:** Directives are currently in force regarding the **Democratic People's Republic of Korea (North Korea)** and the **Islamic Republic of Iran**.
* **Operational Requirement:** Banks must treat **all** transactions originating from or destined to these jurisdictions as **high risk**. This mandates Enhanced Due Diligence (EDD) and verification of the source of funds. Given the risk, most major banks effectively block all direct financial interaction with these states.43

### 5.3 Russian Sanctions (SEMA)

Since 2014, and escalating significantly in 2022, the *Special Economic Measures (Russia) Regulations* have imposed complex prohibitions.

* **Dealings Ban:** It is prohibited for any person in Canada (including banks) to deal in any property held by a designated person or to provide financial services to them.
* **Sectoral Sanctions:** Prohibitions exist on dealing in new debt or equity of certain Russian entities (energy and finance sectors). This requires banks to carefully screen investment banking activities and new bond issuances.46
* **"Arms and Related Material":** Sanctions also prohibit financial services related to the supply of arms. The definition of "arms" is broad, including technical data and chemicals, requiring vigilance in Trade Finance departments.47

## 6. Operational Processes: The Mechanics of Movement

Beyond the legislative requirements, banks utilize specific operational processes to ensure the integrity of the financial system.

### 6.1 The Travel Rule and Payment Systems

The "Travel Rule" is a requirement designed to ensure transparency in the payment chain. It prevents funds from moving anonymously through the banking system.

* **The Requirement:** When a bank initiates an Electronic Funds Transfer (EFT) or Virtual Currency transfer, it must pass specific information to the next financial institution in the chain.
* **Required Data:**
  + Originator's Name, Address, and Account Number.
  + Beneficiary's Name and Address.
* **Incoming Transfers:** If a bank receives a wire that is missing this information, it must take "reasonable measures" to obtain it. This might involve querying the sending bank. If the information is consistently missing, the bank must consider rejecting the transfer or terminating the relationship with the counterparty bank.48

**Lynx and LVTS:**

In Canada, high-value payments move through Lynx (formerly the Large Value Transfer System or LVTS), operated by Payments Canada. Lynx is a Real-Time Gross Settlement (RTGS) system designated as systemically important.

* **ISO 20022:** Lynx supports the **ISO 20022** messaging standard, which allows for "rich data" to travel with the payment. This technical capability helps banks comply with the Travel Rule by providing dedicated fields for originator and beneficiary data, reducing the need for manual truncation or formatting issues common in older MT103 messages.50

### 6.2 Transaction Monitoring and Indicators

Banks employ sophisticated software (e.g., Nice Actimize, Oracle Mantas) to monitor transactions for "Red Flags" or "ML Indicators." These indicators serve as the trigger for an analyst to investigate and potentially file an STR.

* **Scenarios & Rules (The Legacy Layer):** These are the "hard" limits.
  + *Example:* Any cash deposit over **$10,000** automatically triggers a Large Cash Transaction Report (LCTR).
  + *Structuring (Smurfing):* Rules to catch multiple deposits of $9,500 across different branches in Toronto.
* **Behavioral Anomaly Detection (The ML Layer):** Instead of a fixed limit, the system builds a "normal" profile for a client.
  + *The "Segment of One":* If a student who usually spends $2,000/month suddenly receives a $50,000 wire from a high-risk jurisdiction, the model flags it as an anomaly relative to their peer group.
* **Graph Analytics (The Network Layer):** Banks now use graph databases to find "hidden" relationships—circular fund flows where Money moves from Person A → B → C → A

### 6.3 The Operational Workflow

When a system flags a transaction, it doesn't go straight to the government. It enters a specialized "Triage and Investigation" funnel:

* **Alert Generation:** The system (e.g., Verafin, Oracle Mantas, or a custom-built AI model) generates an alert.
* **Level 1 (Triage):** Usually handled by a large team of junior analysts or an **AI Triage Model**. They filter out "False Positives" (e.g., a legitimate business getting a seasonal spike in sales).
* **Level 2 (Investigation):** Senior analysts conduct a "Deep Dive." They look at the client's KYC (Know Your Customer) file, check for "Adverse Media" (news stories), and look at the "counterparty" (who sent/received the money).
* **The STR Decision:** If they have **"Reasonable Grounds to Suspect"** (the legal threshold in Canada), they file a **Suspicious Transaction Report (STR)** to FINTRAC.

### 

### 

### 

### 

### 

### 

### 6.4 Top AML Alert Rules & Models

* **Structuring/Smurfing:** Multiple transactions just under the $10,000 threshold within a short period.
* **Rapid In-and-Out (Pass-Through):** Funds deposited and immediately wired out to a different account.
* **High-Risk Jurisdiction Flow:** Large or frequent transfers to/from countries with weak AML regimes or high sanctions risk.
* **Peer Group Anomaly:** Activity that deviates significantly from the "normal" behavior of similar demographic profiles.
* **U-Turn Transactions:** Funds that leave an account and eventually return from a different source (Circular Flow).
* **Dormant Account Reactivation:** Sudden high-volume activity on an account that has been inactive for months.
* **Frequent Small e-Transfers:** A high volume of Interac e-Transfers that mimics retail business activity in a personal account.
* **Merchant Category Code (MCC) Mismatch:** Corporate card spending on high-risk categories (e.g., casinos, jewelry) inconsistent with the business type.
* **Pass-Through Accounts:** A classic indicator where an account receives funds and immediately wires them out to a foreign jurisdiction, leaving a near-zero balance. The account serves no economic purpose other than layering funds.53
* **Velocity of Funds:** Money moving faster than the client's profile suggests is normal (e.g., a student account moving $100,000 in a week).
* **Underground Banking Indicators:** Transfers from unrelated third parties, use of bank drafts to settle debts with no clear source, or funds coming from MSBs in high-risk jurisdictions (like Hong Kong) with no clear business rationale.56

## 7. Public-Private Partnerships: Intelligence-Led Compliance

A defining feature of the modern Canadian regime is the collaboration between FINTRAC, law enforcement, and the private sector (banks). This is operationalized through "Projects"—public-private partnerships (PPPs) targeting specific types of crime.

### 7.1 Project Protect (Human Trafficking)

Launched in 2016, this was the first major PPP. It focuses on money laundering associated with human trafficking in the sex trade.

* **Indicators:** Banks look for specific red flags such as purchases of online ads on classified sites (e.g., Leolist), hotel bookings in varying cities over short periods, late-night ride-share transactions, and excessive cash deposits.
* **Action:** STRs filed under this project are tagged (e.g., "#PROTECT") to fast-track them to police units specializing in trafficking.1

### 7.2 Project Shadow (Online Child Exploitation)

This project focuses on the financial footprint of purchasing Child Sexual Abuse Material (CSAM) and the laundering of proceeds from its sale.

* **Indicators:** Low-value transactions to known streaming or content platforms associated with CSAM, or use of specific keywords in payment fields. The goal is to identify perpetrators and rescue victims.58

### 7.3 Project Athena / Laundromat (Underground Banking)

Targeting professional money laundering, specifically the "Vancouver Model." This involves underground banking schemes where funds are moved informally (e.g., a gambler borrows cash in Vancouver from a loan shark and repays via a bank transfer in China).

* **Indicators:** Banks look for anomalies in bank drafts (e.g., drafts purchased with cash by third parties), funds from unknown sources paying off credit lines, and transactions involving casino markers.56

### 7.4 Project Chameleon (Romance Fraud)

Focuses on victims (often seniors) being coerced into sending money to fraudsters they have met online.

* **Indicators:** Sudden changes in spending patterns of elderly clients, transfers to high-risk jurisdictions (e.g., Nigeria, Ghana, Turkey) inconsistent with the client's history, or the liquidation of investment products to fund wire transfers.1

### 7.5 Project Guardian (Fentanyl/Opioids)

Aimed at combatting the laundering of proceeds from the trafficking of illicit fentanyl.

* **Indicators:** Transactions involving chemical supply companies, payments to jurisdictions known for precursor chemical production, and cash activity consistent with drug dealing.60

### 7.6 Project Anton (Illegal Wildlife Trade)

The newest project, targeting the laundering of proceeds from the illegal wildlife trade.

* **Indicators:** Transactions involving import/export businesses dealing in high-risk fauna/flora, payments to wildlife risk jurisdictions, and inconsistencies in shipping documentation.61

## 8. Enforcement and Remediation

When banks fail to meet their obligations, the consequences are severe. The regime uses a graduated enforcement approach, ranging from feedback to criminal prosecution.

### 8.1 Administrative Monetary Penalties (AMPs)

FINTRAC has the authority to issue Administrative Monetary Penalties (AMPs) for non-compliance. These are not criminal charges but civil penalties.

* **Calculation:** The penalty amount depends on the "harm" done to the regime and the entity's history of compliance.
* **Naming and Shaming:** Crucially, FINTRAC now publicly names entities that receive AMPs. For a Big 5 bank, the reputational damage of being "named" often outweighs the financial cost of the fine.3

### 8.2 Voluntary Self-Declaration of Non-Compliance (VSDONC)

If a bank discovers it has breached the act (e.g., a coding error caused 5,000 LCTRs to be missed over the last year), it acts in its favor to self-report.

* **The Mechanism:** The bank submits a VSDONC to FINTRAC in writing, detailing the issue, the number of reports impacted, and the remediation plan.64
* **The Benefit:** While not a "get out of jail free" card, FINTRAC considers the voluntary nature of the disclosure when determining if a penalty is warranted. A proactive VSDONC demonstrates a robust compliance culture and may lead to a reduced penalty or no penalty at all.

### 8.3 Criminal Non-Compliance

For egregious cases—such as knowingly failing to report suspicious transactions or destroying records to hide evidence—the PCMLTFA provides for criminal sanctions. FINTRAC can disclose information to law enforcement to support the investigation of these non-compliance offenses.66

#### Works cited

1. Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime Strategy 2023-2026, accessed November 21, 2025, <https://www.canada.ca/en/department-finance/programs/financial-sector-policy/canadas-anti-money-laundering-and-anti-terrorist-financing-regime-strategy-2023-2026.html>
2. AML/ATF Statement - SBI Canada Bank, accessed November 21, 2025, <https://ca.statebank/documents/344623/345264/AML-ATF+Statement+%281%29.pdf/b74f9ff7-25d0-bd96-f0ba-3b55dd04ebec?t=1615933003622>
3. Proceeds of Crime (Money Laundering) and Terrorist Financing Act - Laws.justice.gc.ca, accessed November 21, 2025, <https://laws-lois.justice.gc.ca/eng/acts/p-24.501/>
4. Proceeds of Crime (Money Laundering) and Terrorist Financing Reporting of Goods Regulations: SOR/2025-67 - Gazette du Canada, accessed November 21, 2025, <https://gazette.gc.ca/rp-pr/p2/2025/2025-03-26/html/sor-dors67-eng.html>
5. Reporting large cash transactions to FINTRAC - canafe - Canada.ca, accessed November 21, 2025, <https://fintrac-canafe.canada.ca/guidance-directives/transaction-operation/lctr-doie/lctr-doie-eng>
6. Beneficial ownership discrepancy reporting - Innovation, Science and Economic Development Canada, accessed November 21, 2025, <https://ised-isde.canada.ca/site/corporations-canada/en/beneficial-ownership-discrepancy-reporting>
7. OSFI Annual Report 2021-22 - Office of the Superintendent of Financial Institutions, accessed November 21, 2025, <https://www.osfi-bsif.gc.ca/en/about-osfi/reports-publications/osfi-annual-report-2021-22>
8. OSFI revises anti-money laundering supervisory approach - DLA Piper, accessed November 21, 2025, <https://www.dlapiper.com/en/insights/publications/2020/11/osfi-revises-anti-money-laundering-supervisory-approach>
9. Mandate - canafe - Canada.ca, accessed November 21, 2025, <https://fintrac-canafe.canada.ca/fintrac-canafe/1-eng>
10. Deterring and Detecting Money Laundering and Terrorist - Gov.bc.ca, accessed November 21, 2025, <https://ag-pssg-sharedservices-ex.objectstore.gov.bc.ca/ag-pssg-cc-exh-prod-bkt-ex/416%20-%20Office%20of%20the%20Superintendent%20of%20Financial%20Institutions%20Canada%20guideline%20Deterring%20and%20Detecting%20Money%20Laundering%20and%20Terrorist%20Finance%20no.%20B-8%20dated%20December%202008.pdf>
11. Compliance program requirements - canafe - Canada.ca, accessed November 21, 2025, <https://fintrac-canafe.canada.ca/guidance-directives/compliance-conformite/guide4/4-eng>
12. Anti-money laundering compliance (Fintrac) - Canadian Home Builders' Association, accessed November 21, 2025, <https://www.chba.ca/anti-money-laundering-compliance-fintrac/>
13. Guidance on the Risk-Based Approach to Combatting Money laundering and Terrorist Financing - à www.publications.gc.ca, accessed November 21, 2025, <https://publications.gc.ca/collections/collection_2017/canafe-fintrac/FD4-6-2016-eng.pdf>
14. Risk assessment guidance - canafe - Canada.ca, accessed November 21, 2025, <https://fintrac-canafe.canada.ca/guidance-directives/compliance-conformite/rba/rba-eng>
15. An Overview of the Five Pillars of a BSA/AML Compliance Program - Alessa, accessed November 21, 2025, <https://alessa.com/blog/five-pillars-of-bsa-aml-compliance-program/>
16. mastering compliance - Gov.bc.ca, accessed November 21, 2025, <https://ag-pssg-sharedservices-ex.objectstore.gov.bc.ca/ag-pssg-cc-exh-prod-bkt-ex/623F%20-%20Mastering%20Compliance%20AMLTraining%20for%20Brokers%20-%20Module%208%20Effectiveness%20Review%20and%20Examinations%20Part%201.pdf>
17. FINTRAC assessment manual: The approach and methods used during examinations, accessed November 21, 2025, <https://fintrac-canafe.canada.ca/guidance-directives/exam-examen/cam/cams-eng>
18. FINTRAC Identification — Canada Verification and KYC Guidelines - Trulioo, accessed November 21, 2025, <https://www.trulioo.com/blog/financial-services/fintrac-identification>
19. Methods to verify the identity of persons and entities - canafe - Canada.ca, accessed November 21, 2025, <https://fintrac-canafe.canada.ca/guidance-directives/client-clientele/guide11/11-eng>
20. Verification of Government-Issued IDs For FINTRAC Compliance - Docusign Support Center, accessed November 21, 2025, <https://support.docusign.com/s/document-item?bundleId=ced1643229641057&topicId=qji1703173387962.html&_LANG=enus>
21. New FinTRAC Guidance - ID Verification - Global Regulation Tomorrow, accessed November 21, 2025, <https://www.regulationtomorrow.com/ca/new-fintrac-guidance-id-verification/>
22. Canada Business Corporations Act new filing requirement and U.S. Corporate Transparency Act coming into effect next year | BD&P, accessed November 21, 2025, <https://www.bdplaw.com/insights/canada-business-corporations-act-new-filing-requirement-and-u-s-corporate-transparency-act-coming-into-effect-next-year>
23. Beneficial ownership requirements - : - FINTRAC's compliance guidance - canafe - Canada.ca, accessed November 21, 2025, <https://fintrac-canafe.canada.ca/guidance-directives/client-clientele/bor-eng>
24. Canada Accelerates Amendments to Its Anti-Money Laundering and Anti-Terrorist Financing Regime | Blakes, accessed November 21, 2025, <https://www.blakes.com/insights/canada-accelerates-amendments-to-its-anti-money-laundering-and-anti-terrorist-financing-regime/>
25. Now in effect: Regulatory updates impacting reporting entities under Canada's AML regime, accessed November 21, 2025, <https://www.dlapiper.com/en/insights/publications/2025/10/regulatory-updates-impacting-reporting-entities-under-canadas-aml-regime>
26. Beneficial Ownership Guide for Canada - Stolen Asset Recovery Initiative, accessed November 21, 2025, <https://star.worldbank.org/sites/default/files/2024-04/Beneficial%20Ownership%20Guide_Canada%202024%20%20.pdf>
27. PIA – Corporations Canada – Beneficial Ownership Transparency, accessed November 21, 2025, <https://ised-isde.canada.ca/site/atip-services/en/references/pia-corporations-canada-beneficial-ownership-transparency>
28. Frequently asked questions about domestic politically exposed persons and heads of international organizations - canafe, accessed November 21, 2025, <https://fintrac-canafe.canada.ca/individuals-individus/faq-pep-eng>
29. Anti-Money Laundering Update: FINTRAC Releases Guidance In Respect of Politically Exposed Persons - McCarthy Tétrault LLP, accessed November 21, 2025, <https://www.mccarthy.ca/en/insights/publications/anti-money-laundering-update-fintrac-releases-guidance-respect-politically-exposed-persons>
30. Politically exposed persons and heads of international organizations guidance - canafe, accessed November 21, 2025, <https://fintrac-canafe.canada.ca/guidance-directives/client-clientele/pep/pep-eng>
31. Politically exposed persons and heads of international organizations guidance for account-based reporting entity sectors - canafe, accessed November 21, 2025, <https://fintrac-canafe.canada.ca/guidance-directives/client-clientele/pep/pep-acct-eng>
32. Guidance on Politically Exposed Persons/ Heads of International Organizations - Federation of Law Societies of Canada, accessed November 21, 2025, <https://flsc.ca/wp-content/uploads/2024/02/Guidance-on-PEPs-v2.pdf>
33. Record keeping requirements for financial entities - canafe - Canada.ca, accessed November 21, 2025, <https://fintrac-canafe.canada.ca/guidance-directives/recordkeeping-document/record/fin-eng>
34. Comply with FINTRAC's Reporting Changes - NICE Actimize, accessed November 21, 2025, <https://www.niceactimize.com/Lists/Brochures/aml_comply_with_fintracs_reporting_changes_brochure.pdf>
35. Reporting transactions to FINTRAC: The 24-hour rule - canafe - Canada.ca, accessed November 21, 2025, <https://fintrac-canafe.canada.ca/guidance-directives/transaction-operation/24hour/1-eng>
36. Upcoming Changes to FINTRAC Reporting Forms: LCTR, STR, EFTR, and CDR - Alessa, accessed November 21, 2025, <https://alessa.com/blog/fintrac-reporting-forms-changes/>
37. Reporting electronic funds transfers to FINTRAC - canafe - Canada.ca, accessed November 21, 2025, <https://fintrac-canafe.canada.ca/guidance-directives/transaction-operation/eft-dt/eft-dt-eng>
38. Reporting large virtual currency transactions to FINTRAC - canafe - Canada.ca, accessed November 21, 2025, <https://fintrac-canafe.canada.ca/guidance-directives/transaction-operation/lvctr/lvctr-eng>
39. What are the FINTRAC requirements for banks in Canada? - Lexpert, accessed November 21, 2025, <https://www.lexpert.ca/news/legal-faq/what-are-the-fintrac-requirements-for-banks-in-canada/392988>
40. Canadian Sanctions - Frequently Asked Questions - Global Affairs Canada, accessed November 21, 2025, <https://www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/faq.aspx?lang=eng>
41. Canadian sanctions legislation - Global Affairs Canada, accessed November 21, 2025, <https://www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/legislation-lois.aspx?lang=eng>
42. Sanctions Regime: Overview (Canada) | Norton Rose Fulbright, accessed November 21, 2025, [https://www.nortonrosefulbright.com/-/media/files/nrf/nrfweb/knowledge-pdfs/sanctions-regime-overview-canadara.pdf?revision=&revision=4611686018427387904](https://www.nortonrosefulbright.com/-/media/files/nrf/nrfweb/knowledge-pdfs/sanctions-regime-overview-canadara.pdf?revision&revision=4611686018427387904)
43. A Primer on Canadian Sanctions Legislation - Blakes, accessed November 21, 2025, <https://www.blakes.com/insights/a-primer-on-sanctions-legislation/>
44. Ministerial directives and transaction restrictions - canafe - Canada.ca, accessed November 21, 2025, <https://fintrac-canafe.canada.ca/obligations/directives-eng>
45. Webinar recording – Sanctions evasion, property reporting and the fight against illegal fentanyl financing - canafe, accessed November 21, 2025, <https://fintrac-canafe.canada.ca/training-formation/sanctions/video-eng>
46. Canadian Sanctions Related to Russia - Global Affairs Canada, accessed November 21, 2025, <https://www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/russia-russie.aspx?lang=eng>
47. Special Economic Measures (Russia) Regulations ( SOR /2014-58) - Laws.justice.gc.ca, accessed November 21, 2025, <https://laws.justice.gc.ca/eng/regulations/sor-2014-58/fulltext.html>
48. Travel rule for electronic funds and virtual currency transfers - canafe - Canada.ca, accessed November 21, 2025, <https://fintrac-canafe.canada.ca/guidance-directives/transaction-operation/travel-acheminement/1-eng>
49. Canada: FINTRAC Guidance on Travel Rule for Electronic Funds & Virtual Currency Transfers 2021 | WTR, accessed November 21, 2025, <https://wtr.opusdatum.com/north-america-guidelines/canada%3A-fintrac-guidance-on-travel-rule-for-electronic-funds-%26-virtual-currency-transfers-2021>
50. An Overview of Lynx, Canada's High-Value Payment System, accessed November 21, 2025, <https://www.bankofcanada.ca/wp-content/uploads/2022/05/Overview-Lynx-Canadas-High-Value-Payment-System.pdf>
51. High-value payment system - Lynx - Payments Canada, accessed November 21, 2025, <https://www.payments.ca/systems-services/payment-systems/high-value-payment-system-lynx>
52. 41. Wire Transfer Best Practices | Canadian Bar Association, accessed November 21, 2025, <https://www.cba.org/resources/practice-tools/mortgage-instructions-toolkit/wire-transfer-best-practices/>
53. Operational Alert: Laundering the proceeds of illicit synthetic opioids - canafe - Canada.ca, accessed November 21, 2025, <https://fintrac-canafe.canada.ca/intel/operation/iso-osi-eng>
54. Money laundering and terrorist financing indicators—Accountants - canafe - Canada.ca, accessed November 21, 2025, <https://fintrac-canafe.canada.ca/guidance-directives/transaction-operation/indicators-indicateurs/accts_mltf-eng>
55. Top 10 AML Red Flags Every Compliance Officer Must Know, accessed November 21, 2025, <https://amlincubator.com/blog/top-10-aml-red-flags-every-compliance-officer-must-know>
56. Updated indicators: Laundering the proceeds of crime through underground banking schemes - canafe, accessed November 21, 2025, <https://fintrac-canafe.canada.ca/intel/operation/ml-rec-eng>
57. FINTRAC - OSCE, accessed November 21, 2025, <https://www.osce.org/files/f/documents/0/b/382174.pdf>
58. Project Shadow - WeProtect Global Alliance, accessed November 21, 2025, <https://www.weprotect.org/resources/case-study/project-shadow/>
59. Operational alert: Laundering of proceeds from online child sexual exploitation - canafe, accessed November 21, 2025, <https://fintrac-canafe.canada.ca/intel/operation/exploitation-eng>
60. FINTRAC provides additional money laundering indicators associated with human trafficking for sexual exploitation in support of Project Protect - canafe, accessed November 21, 2025, <https://fintrac-canafe.canada.ca/new-neuf/nr/2021-07-30-eng>
61. FINTRAC publishes money laundering indicators related to illegal wildlife trade in support of Project Anton - Canada.ca, accessed November 21, 2025, <https://www.canada.ca/en/financial-transactions-reports-analysis/news/2023/01/fintrac-publishes-money-laundering-indicators-related-to-illegal-wildlife-trade-in-support-of-project-anton.html>
62. READOUT: FinCEN and Partner FIU Officials Meet in Canada for International Public-Private Partnership Events on Illicit Finance, accessed November 21, 2025, <https://www.fincen.gov/news/news-releases/readout-fincen-and-partner-fiu-officials-meet-canada-international-public>
63. FINTRAC introduces tools to assist reporting entities with AML obligations, accessed November 21, 2025, <https://www.regulationtomorrow.com/ca/fintrac-introduces-tools-to-assist-reporting-entities-with-aml-obligations/>
64. Voluntary self-declaration of non-compliance - canafe - Canada.ca, accessed November 21, 2025, <https://fintrac-canafe.canada.ca/guidance-directives/exam-examen/vsdonc/1-eng>
65. Voluntary self-declaration of non-compliance form - canafe - Canada.ca, accessed November 21, 2025, <https://fintrac-canafe.canada.ca/notices-avis/vsdonc-form-eng>
66. Assessment and enforcement - canafe - Canada.ca, accessed November 21, 2025, <https://fintrac-canafe.canada.ca/assess-eval/1-eng>