# Navigating the Shift: An Exhaustive Analysis of Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime

## Executive Summary

Canada's Anti-Money Laundering and Anti-Terrorist Financing (AML/ATF) regime is undergoing a period of unprecedented and accelerated transformation. Anchored by the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA) and supervised by the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), the framework has evolved from a conventional reporting system into a dynamic and increasingly punitive regulatory ecosystem. This report provides an exhaustive analysis of this regime, dissecting its legal architecture, the operational duties it imposes on regulated businesses, the severe consequences of non-compliance, and the critical implications of a recent wave of sweeping legislative amendments.

The core themes of this analysis reveal a complex, interconnected system. The PCMLTFA serves as an administrative law superstructure built upon a criminal law foundation, with its effectiveness critically dependent on the quality and timeliness of reporting from a wide range of private sector entities. These Reporting Entities (REs) are mandated to implement and maintain a robust, risk-based compliance program structured around five key pillars: a designated compliance officer, comprehensive policies and procedures, a tailored risk assessment, ongoing training, and a biennial effectiveness review.

Enforcement has intensified dramatically. FINTRAC is now wielding its authority to levy multi-million dollar Administrative Monetary Penalties (AMPs) and is legally required to publicly name all violators. This has elevated compliance from a background regulatory concern to a critical business and reputational imperative. A failure to comply is no longer a private matter between a business and its regulator; it is a public event with significant financial and brand repercussions.

Most significantly, a wave of amendments enacted and proposed between 2023 and 2025, driven by both international pressure from the Financial Action Task Force (FATF) and urgent domestic priorities, is fundamentally reshaping the landscape. These changes are expanding the regime's scope to new sectors, increasing compliance burdens, enhancing transparency requirements around beneficial ownership, and introducing novel cooperative mechanisms, such as private-to-private information sharing, to combat financial crime.

In this new environment, a reactive or minimalist approach to compliance is untenable. Proactive, strategic, and well-resourced compliance is no longer merely a regulatory requirement but a cornerstone of sound risk management, corporate governance, and sustainable business operations for any entity participating in Canada's financial system.

## Section 1: The Legislative and Regulatory Cornerstone: PCMLTFA and Complementary Statutes

Canada's AML/ATF regime is a multi-layered legal framework designed to protect the integrity of the national and global financial systems. While the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* is the central pillar, it does not operate in isolation. It functions as a comprehensive administrative law system built upon a foundation of criminal law, drawing strength and scope from the *Criminal Code of Canada* and an expanding array of sanctions legislation. Understanding this interconnected architecture is fundamental to appreciating the depth and breadth of the obligations imposed on regulated entities.

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

The PCMLTFA is the primary statute governing Canada's AML/ATF efforts. Enacted in 2000 as the *Proceeds of Crime (Money Laundering) Act* and significantly amended in 2001 to include terrorist financing measures, the Act establishes a framework of detection, deterrence, and investigation.

#### Core Objectives

As articulated in Section 3 of the Act, the PCMLTFA has a clear, fourfold purpose that guides its application and enforcement. First, it seeks to implement specific, practical measures to detect and deter money laundering and the financing of terrorist activities. This is achieved by imposing mandatory record-keeping, client identification, and reporting requirements on a wide array of businesses susceptible to misuse by criminals. Second, the Act aims to respond to the threat posed by organized crime by providing law enforcement officials with the financial intelligence necessary to trace and deprive criminals of their illicit profits. Third, it serves to fulfill Canada's international commitments to participate in the global fight against transnational crime. Finally, it is designed to enhance Canada's capacity to take targeted measures to protect its financial system from abuse, thereby mitigating the risk of it being used as a conduit for illicit funds.

#### Legislative Architecture

The PCMLTFA is structured into several key parts, each serving a distinct function in achieving its overarching objectives. This structure creates a logical flow from the imposition of duties on the private sector to the establishment of the regulator and the mechanisms for enforcement.

* **Part 1 and 1.1** form the operational core of the Act for most businesses. Part 1 imposes the foundational obligations on REs, including the requirements to keep records, verify client identity, report specific types of transactions, and, for certain sectors like Money Services Businesses (MSBs), register with FINTRAC. Part 1.1 grants the Minister of Finance the power to issue directives and regulations to take countermeasures against threats to the integrity of Canada's financial system, such as those emanating from high-risk foreign jurisdictions.
* **Part 2 and 2.1** address the physical movement of value across borders. Part 2 establishes the rules for reporting the cross-border movement of currency and monetary instruments exceeding $10,000. Part 2.1, a more recent addition, extends similar reporting obligations to the cross-border movement of goods, targeting trade-based money laundering.
* **Part 3** establishes the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). It defines the Centre's object, powers, organizational structure, and operational framework as both a supervisor and a financial intelligence unit.
* **Part 4 and 4.1** provide the regulatory and enforcement authority. Part 4 grants the government the power to create the detailed regulations that give practical effect to the Act's high-level requirements. Part 4.1 establishes the legal framework for the Administrative Monetary Penalties (AMPs) program, which is FINTRAC's primary civil enforcement tool.
* **Part 5** outlines specific criminal offences and punishments for non-compliance with the PCMLTFA itself, such as failing to report suspicious transactions or "tipping off" a client that a report has been filed. These are distinct from the underlying money laundering offences in the *Criminal Code*.

#### Associated Regulations

The PCMLTFA is a framework statute, with the specific, granular rules of compliance contained within a suite of associated regulations. These regulations are essential reading for any RE, as they detail the "how-to" of compliance. Key regulations include :

* *Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations:* The main set of rules covering client identification, record-keeping, and threshold transaction reporting.
* *Proceeds of Crime (Money Laundering) and Terrorist Financing Suspicious Transaction Reporting Regulations:* Specifies the content and form for Suspicious Transaction Reports (STRs) and Terrorist Property (TP) reports.
* *Proceeds of Crime (Money Laundering) and Terrorist Financing Administrative Monetary Penalties Regulations:* Lists the specific violations that can lead to an AMP and classifies their severity.
* Other regulations cover cross-border currency reporting, MSB registration, and the new assessment of expenses model for funding FINTRAC's compliance activities.

### 1.2 The Criminal Code of Canada: The Predicate Offences

The entire PCMLTFA regime is designed to combat specific crimes defined elsewhere, primarily in the *Criminal Code of Canada*. These are the "predicate offences" whose proceeds criminals seek to launder or whose activities they seek to fund.

#### Money Laundering Offence (s. 462.31)

Section 462.31 of the *Criminal Code* defines the act of money laundering in Canada. An offence is committed when a person "uses, transfers the possession of, sends... disposes of or otherwise deals with... any property or any proceeds of any property" derived from a "designated offence." This action must be done with the dual mental element (*mens rea*) of intending to conceal or convert the property, while knowing, believing, or being reckless as to its illicit origins. The scope is exceptionally broad, as a "designated offence" includes a vast range of indictable crimes in Canada. The penalties are severe: up to ten years imprisonment for a standard offence, rising to a maximum of 14 years if the laundering is done for the benefit of, at the direction of, or in association with a criminal organization.

This legal structure establishes a critical distinction: the *Criminal Code* criminalizes the act of laundering itself, while the PCMLTFA creates a regulatory regime to help detect and deter that act. The information collected by REs under the PCMLTFA is ultimately intended to provide law enforcement with the evidence needed to secure a conviction under section 462.31. This relationship demonstrates that an RE's compliance failure is not merely an administrative breach; it is a failure that directly impedes the state's ability to investigate and prosecute serious organized crime. This understanding contextualizes the increasing severity of penalties for non-compliance, as they are seen as proportionate to the harm caused to the criminal justice system.

#### Terrorist Financing Offences (Part II.1, ss. 83.02-83.04)

Part II.1 of the *Criminal Code* contains the offences related to the financing of terrorism. Specifically, sections 83.02, 83.03, and 83.04 make it a serious crime to, directly or indirectly, provide, make available, or collect property with the intention or knowledge that it will be used to facilitate or carry out a terrorist activity. These sections provide the legal foundation for the "terrorist financing" component of the AML/ATF regime, defining the criminal conduct that the PCMLTFA's reporting and due diligence measures are designed to uncover.

### 1.3 The Broader Legal Ecosystem: Sanctions and Related Acts

The Canadian AML/ATF landscape has been significantly complicated by the recent and explicit integration of Canada's economic sanctions regime into the PCMLTFA's reporting framework. This move has expanded the compliance perimeter for all REs, transforming sanctions screening from a related but often separate function into a core component of AML/ATF obligations.

#### Integration with Sanctions Regimes

Amendments to the PCMLTFA and its regulations now require REs to file specific reports related to sanctions. This includes filing a Listed Person or Entity Property Report upon identifying property controlled by a sanctioned party. Crucially, REs must also file an STR if they have reasonable grounds to suspect a transaction is related to *sanctions evasion*. This creates a direct link between a failure in sanctions compliance and a violation of the PCMLTFA.

This integration presents a formidable challenge. Canada's sanctions regime is complex, changes frequently, and, as noted by legal experts, suffers from a lack of comprehensive government guidance. The "deemed ownership" rules, for instance, can render an entity sanctioned even if it does not appear on any official list, making robust screening exceptionally difficult. By weaving these complex and often opaque obligations into the PCMLTFA, the government has significantly increased the compliance burden and risk for REs. A failure to adequately screen for sanctioned entities or detect sanctions evasion can now directly expose an RE to FINTRAC's powerful enforcement toolkit, including substantial AMPs and public naming.

#### Key Sanctions Legislation

As a result of this integration, REs must now be familiar with the primary statutes that underpin Canada's sanctions lists as part of their broader AML/ATF compliance program. These include :

* The *Special Economic Measures Act (SEMA)*
* The *United Nations Act*
* The *Justice for Victims of Corrupt Foreign Officials Act (Sergei Magnitsky Law)*

## Section 2: The Central Authority: Mandate and Operations of FINTRAC

The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) is the independent government agency at the heart of the country's AML/ATF regime. Established in 2000 by the PCMLTFA, FINTRAC is a unique entity with a complex dual mandate: it is simultaneously the primary supervisor responsible for ensuring private sector compliance and Canada's national financial intelligence unit (FIU) responsible for generating actionable intelligence for law enforcement and national security agencies. Operating at arm's length from the police and other investigative bodies, FINTRAC reports to the Minister of Finance, who is in turn accountable to Parliament for its activities.

### 2.1 FINTRAC's Dual Mandate: Supervisor and Financial Intelligence Unit (FIU)

Understanding FINTRAC requires appreciating the distinct yet intertwined nature of its two primary functions. This duality shapes its interactions with REs and defines its position within the broader security apparatus.

#### The Supervisor Role

In its capacity as a supervisor, FINTRAC's core responsibility is to ensure that the thousands of REs across Canada's diverse economic sectors are complying with their obligations under the PCMLTFA and its associated regulations. These sectors include financial entities, securities dealers, life insurance companies, real estate brokers, casinos, MSBs, accountants, and dealers in precious metals and stones, among others. To fulfill this supervisory mandate, FINTRAC undertakes several key activities:

* **Examinations:** FINTRAC conducts risk-based compliance assessments—known as examinations—of REs to verify that their compliance programs are in place and effective. These can be desk-based reviews or more intensive on-site visits.
* **Guidance and Outreach:** The Centre issues extensive guidance, policy interpretations, and learning resources to help REs understand and implement their complex obligations. It also engages in sector-specific consultations to refine its guidance.
* **Registration:** FINTRAC is responsible for maintaining a public registry of all MSBs and foreign MSBs operating in Canada, a key control measure for a high-risk sector.
* **Enforcement:** When non-compliance is identified, FINTRAC has a range of enforcement tools at its disposal, the most significant of which is the power to issue AMPs.

#### The Financial Intelligence Unit (FIU) Role

As Canada's FIU, FINTRAC serves as the central hub for collecting and analyzing financial transaction data to produce intelligence on money laundering, terrorist financing, and threats to the security of Canada. This function is the ultimate purpose of the entire reporting regime. Key activities in this role include:

* **Receiving Reports:** FINTRAC receives millions of financial transaction reports from REs each year, including STRs, Large Cash Transaction Reports (LCTRs), and Electronic Funds Transfer (EFT) reports.
* **Analysis:** Using sophisticated analytical tools and drawing on a wide variety of information sources, FINTRAC analysts sift through this vast dataset to detect patterns, uncover hidden networks, and follow the trail of illicit money. The goal is to piece together disparate transactions to form a coherent intelligence picture.
* **Disclosure:** When FINTRAC's analysis establishes "reasonable grounds to suspect" that specific information would be relevant to the investigation or prosecution of a money laundering or terrorist financing offence, it produces a disclosure of "actionable financial intelligence." This intelligence package is then provided to the appropriate domestic law enforcement or national security agency, or to a foreign FIU partner.

The dual mandate of supervisor and FIU creates a complex operational reality. As a supervisor, FINTRAC often seeks to be a partner, educating REs to foster a culture of compliance. However, as an FIU, its focus is on enforcement and generating intelligence for prosecution. This can create an inherent tension in its relationship with REs, which must simultaneously see the agency as a source of guidance and as a powerful enforcer. The recent trend towards more frequent and severe penalties suggests the balance is increasingly tilting towards a more assertive, enforcement-focused posture, requiring REs to engage with the Centre with a clear-eyed understanding of this asymmetrical power dynamic.

### 2.2 The Flow of Information: From Reporting to Disclosure

The effectiveness of Canada's AML/ATF regime hinges on a continuous intelligence cycle that begins with the private sector and culminates in law enforcement action.

1. **Submission:** The cycle begins when an RE identifies a transaction that meets a reporting threshold. For example, an employee at a financial institution may identify a series of unusual transactions, and after an internal assessment, the institution's compliance officer concludes there are reasonable grounds to suspect money laundering. An STR is then compiled and submitted to FINTRAC through a secure electronic reporting system.
2. **Collection and Analysis:** The submitted report enters FINTRAC's secure databases. There, analysts can link it with other reports from different REs, information from law enforcement, publicly available information, and intelligence from foreign partners. This process of data fusion allows analysts to identify previously unknown links between individuals, accounts, and criminal activities.
3. **Disclosure:** If the cumulative analysis meets the legal disclosure threshold, FINTRAC prepares a detailed intelligence case. This is not raw data but a curated intelligence product that explains the suspected illicit activity and the financial trail. This package is then disclosed to the appropriate partner agency.
4. **Investigation:** The recipient agency—for example, the RCMP—uses FINTRAC's intelligence as a crucial lead. It can provide the basis for obtaining production orders, search warrants, and ultimately, laying criminal charges under the *Criminal Code*.

This entire process is predicated on the **arm's length principle**. FINTRAC itself does not conduct criminal investigations or lay charges. Its role is strictly to provide intelligence to the bodies that do. This separation is a key feature of the Canadian model, designed to protect privacy and ensure a clear division of responsibilities.

The critical dependency of this entire cycle on the initial reports from REs cannot be overstated. FINTRAC cannot analyze what it does not receive. A poorly written STR that lacks detail, a delayed LCTR, or a missed STR altogether can break a vital link in an investigation, allowing criminal networks to continue operating undetected. This dependency explains FINTRAC's intense focus on the quality and timeliness of reporting during its compliance examinations and justifies the severe penalties for reporting violations. From the regulator's perspective, a failure to report is a failure that causes a "complete loss of financial information," directly undermining the core mandate of the entire regime.

### 2.3 Domestic and International Cooperation

Given that money laundering and terrorist financing are overwhelmingly transnational crimes, cooperation is essential to FINTRAC's mission.

#### Domestic Partners

FINTRAC sits at the center of a constellation of domestic partners, each with a specific role in the AML/ATF regime. Key partners include:

* **Law Enforcement:** The Royal Canadian Mounted Police (RCMP) and various provincial and municipal police services are the primary recipients of FINTRAC's intelligence disclosures for criminal investigations.
* **National Security:** The Canadian Security Intelligence Service (CSIS) receives disclosures relevant to threats to the security of Canada, such as terrorism, espionage, and foreign-influenced activities.
* **Other Government Agencies:** FINTRAC also shares information with the Canada Revenue Agency (CRA) for investigations into tax evasion linked to proceeds of crime, the Canada Border Services Agency (CBSA) for cross-border currency and goods enforcement, and prudential regulators like the Office of the Superintendent of Financial Institutions (OSFI) to identify weaknesses in a financial institution's risk controls.

#### International Network

FINTRAC is an active and important player on the global stage. It is a member of the **Egmont Group**, an international network of over 160 FIUs that facilitates the secure exchange of information and intelligence across borders, which is vital for tracing international money flows. FINTRAC also participates in key international policy-setting bodies, including the **Financial Action Task Force (FATF)**, the Asia-Pacific Group on Money Laundering (APG), and the Caribbean Financial Action Task Force (CFATF). This involvement ensures Canada's regime stays aligned with evolving global standards and allows Canada to contribute to the development of those standards.

### 2.4 The Privacy Imperative

The nature of FINTRAC's work necessitates the collection and analysis of vast quantities of sensitive personal financial information. Consequently, the protection of this information is a fundamental and overarching consideration in all of its operations. The PCMLTFA itself contains stringent privacy protection provisions, and any unauthorized use or disclosure of information by FINTRAC personnel is a serious criminal offence, punishable by fines of up to $500,000 and imprisonment for up to five years.

FINTRAC is also subject to the federal *Privacy Act*, which governs how government institutions collect, use, and disclose personal information. However, there is an inherent tension between the agency's mandate to cast a wide net for intelligence and the privacy rights of Canadians. This tension has been highlighted in past audits by the Office of the Privacy Commissioner of Canada (OPC), which criticized FINTRAC for retaining data that was not strictly relevant to its mandate. This balancing act—between the need for broad data analysis to find the "needles in the haystack" of criminal activity and the duty to protect the privacy of the haystack—remains a defining challenge for the agency.

## Section 3: The Five Pillars of Compliance: A Deep Dive into Program Requirements

Under the PCMLTFA and its regulations, every RE is required to develop, implement, and maintain a compliance program. This program is the foundation upon which all other obligations rest. A failure to establish and implement an effective program is itself a serious violation. FINTRAC guidance clearly outlines that a compliant program must be built upon five essential pillars. These pillars are not merely a checklist; they are interconnected components of a comprehensive risk management framework that must be tailored to the specific nature, size, and complexity of the RE's business.

### 3.1 Pillar 1: The Compliance Officer

The first pillar is the appointment of a single individual as the compliance officer. This person is formally responsible for the overall implementation and oversight of the compliance program. To be effective, the compliance officer must be knowledgeable about the PCMLTFA and its requirements and must be given sufficient authority and resources to perform their duties. This includes having access to all relevant information within the organization and the ability to report directly to senior management on the state of the compliance program.

### 3.2 Pillar 2: Policies and Procedures

REs must develop and apply written compliance policies and procedures that are kept up to date and approved by a senior officer. These documents are the operational playbook for the organization's AML/ATF efforts. They must clearly outline how the RE will meet all of its legal obligations, including, at a minimum, its processes for:

* Client identification and verification.
* Third-party determination.
* Ongoing monitoring of business relationships.
* Risk assessment and mitigation.
* Reporting of STRs, LCTRs, EFTs, and other prescribed transactions.
* Record-keeping and retention.
* Applying Ministerial Directives.

The importance of this pillar is underscored by FINTRAC's enforcement actions. An analysis of AMPs issued between 2020 and early 2025 revealed that 63% of penalized entities had deficiencies related to their policies and procedures. The most common failure was the lack of documented or implemented procedures for the ongoing monitoring of business relationships.

### 3.3 Pillar 3: The Risk-Based Approach (RBA) and Assessment

The cornerstone of a modern AML/ATF program is the Risk-Based Approach (RBA). This requires an RE to conduct and document a comprehensive assessment of its business to understand its unique exposure to money laundering and terrorist financing risks. The purpose of the RBA is to allow the RE to apply its compliance resources most effectively, focusing enhanced measures on high-risk areas while applying standard measures to lower-risk areas.

This RBA is, however, a double-edged sword. While it provides flexibility and avoids a rigid, one-size-fits-all model, it also introduces significant ambiguity. The adequacy of an RE's risk assessment is ultimately a matter of regulatory judgment, and FINTRAC's enforcement record shows a major disconnect between what many REs consider adequate and what the regulator expects. Like policy and procedure failures, 63% of penalized entities had an inadequate risk assessment, making it one of the most common and critical compliance failures.

According to FINTRAC guidance, a compliant risk assessment must consider and document how the RE evaluates the risks associated with :

1. **Clients and Business Relationships:** The nature of the RE's clientele, their typical transaction patterns, and their geographic locations.
2. **Products, Services, and Delivery Channels:** The specific offerings of the RE and how they are delivered (e.g., face-to-face, online, through agents).
3. **Geographic Locations:** The regions where the RE conducts its activities.
4. **New Developments and Technologies:** The risks associated with new products or the adoption of new technologies for service delivery or compliance.
5. **Other Relevant Factors:** Any other internal or external factors that could affect the business's risk profile.

A deficient risk assessment is a foundational failure that cascades through the entire compliance program. If risks are not properly identified and assessed, the policies designed to mitigate them will be ineffective, client risk ratings will be inaccurate, and ongoing monitoring will be miscalibrated. For this reason, the RBA is the single greatest point of vulnerability for an RE during a FINTRAC examination.

### 3.4 Pillar 4: Training Program

An RE must develop and maintain a written, ongoing training program for all employees, agents, and any other individuals authorized to act on its behalf. The purpose of the training is to ensure that everyone understands their responsibilities under the law and the organization's internal policies and procedures. The training plan should be tailored to the business and to specific roles within it, and it must be reviewed and updated regularly to reflect changes in the law and the business's risk environment.

### 3.5 Pillar 5: The Two-Year Effectiveness Review

The final pillar is the requirement to conduct a review of the compliance program, at least every two years, to test its effectiveness. This review must assess the performance of the policies and procedures, the risk assessment, and the training program. It can be conducted by either an internal or external auditor. The key is that the review must be comprehensive and its results must be documented, including any identified deficiencies, the corrective measures taken, and a timeline for their implementation.

Viewing this review as a mere procedural chore is a strategic error. It is the primary mechanism for an RE to proactively identify and remedy the same weaknesses that a FINTRAC examiner would target. A well-documented effectiveness review that leads to tangible program improvements can be a powerful mitigating factor in an actual examination. It provides concrete evidence of a positive compliance culture and a good-faith effort to meet obligations, which can be crucial when FINTRAC is determining the appropriate enforcement response to any identified non-compliance.

| Pillar | Requirement | Key Considerations / Best Practices | Common Deficiencies (from AMP data ) |
| --- | --- | --- | --- |
| **1. Compliance Officer** | Appoint a single individual responsible for implementing the program. | Must have knowledge, authority, and resources. Should have direct access to senior management. | N/A (Failure to appoint is a foundational violation). |
| **2. Policies & Procedures** | Develop and apply written, up-to-date, and senior-officer-approved policies and procedures covering all obligations. | Must be a living document, tailored to the business, and easily accessible to all staff. Must translate legal requirements into clear operational steps. | Failure to document or implement adequate ongoing monitoring measures. Deficiencies in policies for third-party determination, record-keeping, and reporting. |
| **3. Risk Assessment** | Conduct and document a risk assessment of the business's exposure to ML/TF risks, considering clients, products, geography, and technology. | The assessment must be comprehensive, well-documented, and defensible. It must be the foundation for the entire risk-based approach. | Inadequate consideration of geographic risks. Failure to consider all products and delivery channels. Insufficient analysis of risks associated with clients and business relationships. |
| **4. Training Program** | Develop and maintain a written, ongoing training program for all relevant staff and agents. | Training should be continuous, role-specific, and updated to reflect new laws, risks, and typologies. Records of who was trained and when must be kept. | N/A (Often cited in conjunction with other failures). |
| **5. Effectiveness Review** | Conduct and document a review of the program's effectiveness at least every two years. | Can be internal or external. Must test all key program elements. Findings and remediation plans must be documented and reported to senior management. | N/A (Failure to conduct the review is a violation). |

## Section 4: Core Operational Duties: Client Identification, Reporting, and Record-Keeping

Beyond the five high-level pillars of the compliance program, the PCMLTFA imposes a set of core, day-to-day operational duties on REs. These duties—client identification, transaction reporting, and record-keeping—are the engine of the AML/ATF regime, generating the raw data and information that FINTRAC analyzes to produce financial intelligence.

### 4.1 Know Your Client (KYC) and Due Diligence

The principle of "Know Your Client" (KYC) is a fundamental tenet of AML/ATF regulation worldwide. It is not a single action but a continuous process of due diligence designed to ensure that an RE has a sufficient understanding of its customers and their financial activities.

* **Identity Verification:** The most basic KYC duty is to verify the identity of persons and entities for certain prescribed activities and transactions. FINTRAC provides detailed, sector-specific guidance on when identity must be verified and the acceptable methods for doing so, which can include reviewing government-issued photo ID, using a credit file, or relying on information held by an affiliate.
* **Beneficial Ownership:** A critical and more complex duty is the requirement to determine and verify the beneficial ownership of corporate or entity clients. This means looking through legal structures like corporations and trusts to identify the natural persons (individuals) who ultimately own or control 25% or more of the entity. This requirement is aimed directly at combating the use of anonymous shell companies to launder money.
* **Third-Party Determination:** REs must take reasonable measures to determine whether their client is conducting a transaction on behalf of a third party. If a third party is involved, the RE must obtain specific identifying information about that individual or entity.
* **Ongoing Monitoring:** KYC is not a one-time event at the start of a business relationship. REs have a duty to conduct ongoing monitoring of their clients' activities throughout the life of the relationship. The purpose is to keep client information up to date and to detect transactions or patterns of activity that are unusual or inconsistent with the RE's knowledge of that client, which could trigger the need to file an STR.
* **High-Risk Clients & PEPs:** The RBA requires that clients posing a higher risk of money laundering or terrorist financing be subjected to enhanced due diligence measures. This includes clients identified as Politically Exposed Persons (PEPs), Heads of International Organizations (HIOs), or family members and close associates of such individuals. Enhanced measures can include obtaining information on the source of funds or wealth and conducting more frequent ongoing monitoring.

These combined duties create a continuous, dynamic cycle of vigilance. Information gathered during initial identity verification informs the client's risk rating, which in turn sets the parameters for ongoing monitoring. The results of that monitoring can then lead to a reassessment of the client's risk profile or trigger a report to FINTRAC. A failure at any point in this cycle—such as an incorrect initial risk rating—can systemically weaken the RE's defenses.

### 4.2 The Reporting Imperative: A Guide to FINTRAC Reports

The reporting obligations are the primary mechanism by which information flows from the private sector to FINTRAC. There are several distinct types of reports, each with its own trigger, timeline, and data requirements.

#### Suspicious Transaction Reports (STRs)

The STR is arguably the most important report in the entire regime. Unlike other reports triggered by objective monetary thresholds, the STR is triggered by a subjective judgment. An RE must submit an STR for any financial transaction—completed or merely attempted—where it has **"reasonable grounds to suspect" (RGS)** that the transaction is related to the commission or attempted commission of a money laundering offence, a terrorist activity financing offence, or, more recently, a sanctions evasion offence.

The RGS threshold is the most high-stakes judgment an RE must make. It is an objective standard, meaning the suspicion must be reasonable to an outside observer with similar expertise, based on an assessment of the facts, the context, and relevant money laundering or terrorist financing indicators. It is a lower threshold than the "reasonable grounds to believe" standard required for police to make an arrest, but higher than a "simple suspicion" or gut feeling. The consequences of getting this judgment wrong are severe. The 2024 Federal Court case involving Norwich Real Estate Services, which saw a $156,750 AMP imposed for failing to file STRs, serves as a stark warning. The regulator viewed the failure to file as a "complete loss of financial information," demonstrating that FINTRAC considers this one of the most serious violations an RE can commit. The case underscores that an RE's internal judgment is subject to regulatory second-guessing with significant financial consequences, making it clear that erring on the side of caution and filing a report is far less risky than failing to do so.

Once RGS is established, the STR must be submitted to FINTRAC **"as soon as practicable"**. This means the report should take priority over other tasks. In time-sensitive situations, such as suspected terrorist financing, FINTRAC encourages expedited submission. Furthermore, the PCMLTFA imposes a strict prohibition on **"tipping off."** An RE must not, under any circumstances, disclose to the client or any other unauthorized person that it has filed or is preparing to file an STR.

#### Threshold Reporting

These reports are triggered by objective monetary thresholds, removing the subjectivity of the STR.

* **Large Cash Transaction Reports (LCTRs):** An RE must report the receipt of $10,000 or more in cash (in any currency) from a client in a single transaction. This also applies if the RE receives two or more cash amounts totaling $10,000 or more within a 24-hour period from or on behalf of the same person or entity (the "24-hour rule").
* **Large Virtual Currency Transaction Reports (LVCTRs):** This is the virtual currency equivalent of the LCTR. An RE must report the receipt of $10,000 or more in virtual currency (e.g., Bitcoin, Ethereum) in a single transaction or in multiple transactions within a 24-hour period.
* **Electronic Funds Transfer (EFT) Reports:** An RE must report the sending or receiving of an international EFT of $10,000 or more in a single transaction, initiated at the request of a client.

#### Property Reporting

This is a distinct reporting stream for situations involving known terrorist or sanctioned property.

* **Terrorist Property (TP) / Listed Person or Entity Property Reports:** If an RE knows that it is in possession or control of property that is owned or controlled by or on behalf of a terrorist or a listed terrorist group, it must immediately report it to both the RCMP and CSIS, and also submit a report to FINTRAC. Recent amendments have expanded this obligation to include property of persons or entities designated under Canada's sanctions laws. This is now done via a "Listed Person or Entity Property Report". This is a knowledge-based report, distinct from the suspicion-based STR.

| Report Type | Triggering Event / Threshold | Reporting Timeline | Key Information Required |
| --- | --- | --- | --- |
| **Suspicious Transaction Report (STR)** | "Reasonable grounds to suspect" the transaction is related to an ML, TF, or sanctions evasion offence. No monetary threshold. | As soon as practicable after RGS is established. | Details of the transaction, the parties involved, and a detailed narrative explaining the grounds for suspicion. |
| **Large Cash Transaction Report (LCTR)** | Receipt of $10,000 or more in cash in a single transaction or within a 24-hour period from the same party. | Within 15 calendar days of the transaction. | Details of the transaction, the person conducting it, and on whose behalf it was conducted. |
| **Large Virtual Currency Transaction Report (LVCTR)** | Receipt of $10,000 or more in virtual currency in a single transaction or within a 24-hour period from the same party. | Within 5 working days of the transaction. | Details of the transaction, sender information, type of VC, and exchange rates. |
| **Electronic Funds Transfer (EFT) Report** | Sending or receiving an international EFT of $10,000 or more at the request of a client. | Within 5 working days of the transfer. | Details of the transfer, originator, and beneficiary information. |
| **Listed Person or Entity Property Report** | Knowledge of possessing or controlling property owned by a terrorist group or a person/entity on a sanctions list. | Immediately/Without delay. | Information about the property, its location, and the listed person or entity involved. |

### 4.3 Record-Keeping Obligations

The final core duty is record-keeping. REs must keep detailed records of transactions, client identification information, and copies of all reports submitted to FINTRAC. The general retention period is a minimum of five years from the date the record was created. These records must be maintained in such a way that they can be provided to FINTRAC in a timely manner, generally within 30 days of a request. This requirement ensures that if FINTRAC or law enforcement needs to conduct a deeper investigation, a clear and comprehensive audit trail exists.

## Section 5: Enforcement and Consequences: Navigating Penalties and Criminal Liability

Canada's AML/ATF regime is backed by a powerful and increasingly active enforcement apparatus. FINTRAC has a broad mandate to assess compliance and impose significant penalties for failures. Beyond the administrative consequences meted out by FINTRAC, non-compliance can also lead to severe criminal liability under both the PCMLTFA and the *Criminal Code*. For REs, understanding the "teeth" of the regime is essential for appreciating the profound financial, reputational, and legal risks of non-compliance.

### 5.1 FINTRAC Examinations and Enforcement Actions

FINTRAC's primary tool for supervising REs is the compliance examination. These assessments are conducted on a risk basis, meaning FINTRAC tends to focus its resources on sectors and individual entities it perceives as posing a higher risk of money laundering or terrorist financing. The examination process can involve desk-based reviews of an RE's documentation or more intrusive on-site visits, which include interviewing the compliance officer and other staff, sampling client files, and testing the RE's transaction monitoring and reporting systems.

Following an examination, FINTRAC will issue a findings letter detailing any identified deficiencies. Depending on the nature and severity of these findings, FINTRAC has a range of options, from requiring a follow-up action plan to, in more serious cases, initiating proceedings to impose an Administrative Monetary Penalty (AMP).

### 5.2 Administrative Monetary Penalties (AMPs)

The AMP program is FINTRAC's most potent civil enforcement tool. While the stated purpose of AMPs is to encourage future compliance rather than to punish past behaviour, the practical impact on a business can be severe.

#### Violation Categories and Penalty Calculation

The *Proceeds of Crime (Money Laundering) and Terrorist Financing Administrative Monetary Penalties Regulations* classify every potential violation of the PCMLTFA and its regulations into one of three categories, each with an escalating penalty range :

* **Minor Violation:** $1 to $1,000 per violation.
* **Serious Violation:** $1 to $100,000 per violation.
* **Very Serious Violation:** $1 to $100,000 per violation for an individual, and $1 to $500,000 per violation for an entity.

When calculating the specific penalty amount within these ranges, the Act requires FINTRAC to take three criteria into account: (1) the harm done by the violation; (2) the RE's previous compliance history; and (3) the non-punitive purpose of the penalty. The "harm done" is a key factor, with FINTRAC assessing harm on a scale from low to highest. For example, a complete failure to report STRs is considered to cause the highest level of harm because it results in a total loss of financial intelligence for the Centre.

The Federal Court's 2024 decision in the *Norwich* case provided important clarity on this process. The Court ruled that FINTRAC must assess each of the three penalty factors distinctly. It cannot, for instance, conflate an RE's good compliance history (a first-time offence) with the non-punitive rationale. The regulator must independently consider what penalty amount is sufficient to encourage compliance without crossing the line into punishment.

#### Public Naming and Enforcement Trends

A pivotal change to the regime now requires FINTRAC to **publicly name** any entity that is issued an AMP. The notice, which details the RE, the nature of its violations, and the penalty amount, is published on FINTRAC's website and remains there for five years. This creates a significant and lasting reputational risk that can be as damaging, or even more so, than the financial penalty itself.

Enforcement data reveals a dramatic escalation in FINTRAC's use of AMPs. Between 2020 and 2024, the total value of penalties imposed increased by a factor of 40. In the 2023-24 fiscal year alone, FINTRAC issued penalties totaling over $26 million. Historically, banks and MSBs have faced the most severe penalties, with the average AMP for banks being over $3 million. This trend demonstrates that while the legal theory of AMPs is "non-punitive," the practical reality for a business facing a multi-million dollar penalty and public shaming is functionally indistinguishable from punishment. This signals a clear strategic shift by the government to use the AMP regime as a powerful deterrent to force behavioral change across entire industries.

While this public naming is painful for the penalized entity, it has created an invaluable public resource for all other REs. Compliance officers can and should systematically review the public AMP notices on FINTRAC's website. These notices provide direct intelligence from the regulator on its enforcement priorities, the most common deficiencies it is finding, and the sectors it is targeting. Analysis of penalties issued up to early 2025 shows that failures related to policies and procedures and inadequate risk assessments are the most common violations cited, and that the real estate, MSB, and banking sectors have been the most frequent targets. By learning from the public mistakes of others, a prudent RE can proactively audit and strengthen its own program to avoid a similar fate.

| Violation Category | Penalty Range (for an Entity) | Examples of Violations | "Harm Done" Assessment Criteria | Key Mitigating / Aggravating Factors |
| --- | --- | --- | --- | --- |
| **Minor** | $1 to $1,000 | Isolated late filing of an LCTR; minor record-keeping omissions. | Low Harm: Poses a limited risk to the objectives of the Act. | Mitigating: Voluntary disclosure, strong cooperation. Aggravating: Repeat minor violations. |
| **Serious** | $1 to $100,000 | Failure to register as an MSB; repeated failure to report LCTRs; inadequate documented risk assessment. | Moderate to High Harm: Significantly impedes FINTRAC's ability to receive/analyze information. | Mitigating: Good compliance history, robust remediation plan. Aggravating: Poor compliance history, obstruction. |
| **Very Serious** | $1 to $500,000 | Systemic failure to report STRs; complete absence of a compliance program; failure to apply Ministerial Directives. | Highest Harm: Completely undermines the objectives of the Act, resulting in a total loss of intelligence. | Mitigating: First-time major offence. Aggravating: Systemic and willful non-compliance across the organization. |

### 5.3 Criminal Liability

In addition to administrative penalties, the AML/ATF regime includes the threat of criminal prosecution for the most serious forms of non-compliance.

* **PCMLTFA Offences:** The Act itself creates several criminal offences. For example, knowingly failing to report an STR or a prescribed threshold transaction, or tipping off a client about an STR, are indictable offences punishable by up to five years in prison and/or significant fines.
* **Criminal Code Offences:** An individual or corporation involved in non-compliance could also be charged with the underlying predicate offences. A conviction for money laundering under section 462.31 of the *Criminal Code* carries a maximum sentence of 14 years when linked to organized crime, while a conviction for terrorist financing can result in life imprisonment. This represents the ultimate legal risk for individuals and entities who move from negligent non-compliance to active complicity in financial crime.

## Section 6: The Evolving Landscape: Analysis of Recent and Forthcoming Amendments (2023-2025)

Canada's AML/ATF regime is in the midst of its most significant overhaul since its inception. A series of legislative and regulatory amendments, introduced and accelerated between 2023 and 2025, are fundamentally reshaping the compliance landscape. These changes are driven by a confluence of factors, including the urgent need to combat new domestic threats like the fentanyl crisis, the imperative to align with evolving global standards set by the FATF, and a strategic decision to move the regime towards a more proactive and collaborative model. For REs, both new and old, navigating this period of rapid change is a paramount challenge.

The accelerated timeline for many of these amendments is a critical factor. The Canadian government has explicitly linked the fast-tracking of these changes to the upcoming mutual evaluation of its AML/ATF regime by the FATF, scheduled to begin in late 2025. A poor rating from this international body can have serious economic and reputational consequences for the country. In prioritizing a successful international review, the government has created a high-risk "compliance crunch" for domestic businesses. This forced rush means many entities, particularly those newly brought into the regime, will struggle to achieve full compliance immediately. While FINTRAC has acknowledged this pressure by promising an initial period of focus on "engagement and outreach" rather than punitive enforcement for new REs, the legal obligations are nonetheless in force. This situation has created a predictable wave of future non-compliance that will likely become a major focus of FINTRAC examinations in 2026 and beyond.

### 6.1 Expansion of the Regime: New Reporting Entities

A key thrust of the recent amendments is the expansion of the PCMLTFA's scope to cover new sectors identified as vulnerable to financial crime. As of April 1, 2025, the following businesses are now classified as REs and are subject to the full suite of AML/ATF obligations :

* **Financing and Leasing Companies:** Entities engaged in financing or leasing property (excluding real estate) for business purposes, passenger vehicles, or any other property valued at $100,000 or more.
* **Factoring Companies:** Entities providing factoring services.
* **Cheque-Cashing Businesses:** Businesses offering cheque-cashing services.

For these newly regulated entities, the challenge is immense. They were required to build and implement a full, five-pillar compliance program—including policies, risk assessments, KYC procedures, and reporting systems—on a highly compressed timeline of just a few months, or in some cases, weeks.

### 6.2 A New Era of Cooperation: Private-to-Private Information Sharing

Perhaps the most philosophically significant change is the creation of a legal framework to permit **private-to-private information sharing**. Effective immediately upon publication in early 2025, amendments to the PCMLTFA now allow REs to voluntarily share personal information about a client with each other, without the client's consent. This sharing is permitted only when it is reasonable for the purpose of detecting or deterring money laundering, terrorist financing, or sanctions evasion, and when seeking consent would compromise those efforts. To ensure privacy is protected, participating entities must develop a Code of Practice for secure information handling, which must be approved by the Office of the Privacy Commissioner.

This change marks a fundamental strategic shift. The traditional AML/ATF model was linear and siloed: REs reported vertically to FINTRAC. This new framework creates the potential for a horizontal intelligence network, allowing financial institutions to collaboratively identify suspicious activity, such as a criminal attempting to structure transactions across multiple banks, before a report is even filed with FINTRAC.

### 6.3 Enhancing Transparency: Beneficial Ownership and Trade-Based Crime

Two other major amendments are aimed at increasing transparency in areas highly vulnerable to abuse.

* **Beneficial Ownership Discrepancy Reporting:** Starting October 1, 2025, REs will have a new reporting obligation related to the federal beneficial ownership registry administered by Corporations Canada. When conducting their own beneficial ownership due diligence, if an RE identifies a material discrepancy between the information it has collected and the information in the federal registry, it will be required to report that discrepancy. This creates a powerful feedback loop, effectively deputizing thousands of REs as active auditors of the registry, which will significantly enhance the accuracy and reliability of this critical transparency tool.
* **Trade-Based Money Laundering (TBML):** New regulations that came into force on April 1, 2025, give the Canada Border Services Agency (CBSA) enhanced authorities to combat TBML. This includes new requirements for importers and exporters to declare whether goods are proceeds of crime and gives the CBSA the power to share information with law enforcement to disrupt the use of international trade as a laundering technique.

### 6.4 Toughening the Stance: Increased Penalties and Cash Restrictions

Finally, legislative changes introduced in 2025 signal a significant hardening of the government's enforcement posture.

* **Massively Increased AMPs:** Bill C-2 proposes a new tiered framework for AMPs with substantially increased maximums. Most notably, the maximum penalty for a "very serious" violation would increase from $500,000 to **$20 million**. This astronomical increase sends an unequivocal message that the government views compliance failures as a threat deserving of penalties that could be existential for some businesses.
* **Prohibition on Large Cash Transactions:** The same bill introduces a new, broad-based offence under the PCMLTFA. It would prohibit any person or entity engaged in business from accepting $10,000 or more in cash in a single transaction or in a series of related transactions. The exceptions are narrow, primarily limited to certain regulated financial institutions. This is a proactive measure designed to "harden the target" by making it much more difficult for criminals to inject large amounts of illicit cash into the legitimate economy.

Together, these amendments represent the most profound evolution of the Canadian AML/ATF regime to date. They are moving the system beyond a passive, report-based model towards a more proactive, networked, and transparent ecosystem where the private sector is enlisted as a more active and collaborative partner in the fight against financial crime.

| Amendment Area | Key Change | Primary Impacted Parties | In-Force Date |
| --- | --- | --- | --- |
| **Expansion of Regime** | Factoring, financing/leasing, and cheque-cashing businesses are now REs with full compliance obligations. | Newly regulated entities in these sectors. | April 1, 2025 |
| **Information Sharing** | REs are permitted to voluntarily share client information with each other to detect/deter financial crime. | All REs, particularly large financial institutions. | Immediately (Early 2025) |
| **Beneficial Ownership** | REs must report material discrepancies between their KYC findings and the federal corporate registry. | All REs dealing with corporate clients. | October 1, 2025 |
| **Trade-Based Crime** | CBSA has enhanced powers and reporting requirements are in place for importers/exporters to combat TBML. | Importers, exporters, customs brokers, logistics companies. | April 1, 2025 |
| **Increased AMPs** | Maximum penalty for a "very serious" violation to be increased to $20 million. | All REs. | Proposed in Bill C-2 (2025) |
| **Cash Restriction** | New offence prohibiting businesses from accepting $10,000 or more in cash for a transaction. | All businesses in Canada, with narrow exceptions. | Proposed in Bill C-2 (2025) |

## Section 7: Strategic Recommendations and Outlook

The Canadian AML/ATF landscape is more complex, more dynamic, and more punitive than ever before. For businesses subject to the PCMLTFA, navigating this environment requires a strategic, proactive, and deeply integrated approach to compliance. A reactive, "check-the-box" mentality is a recipe for failure, risking severe financial penalties, lasting reputational damage, and, in the most serious cases, criminal liability.

### 7.1 Actionable Recommendations for Compliance Programs

In light of the analysis presented in this report, REs should consider the following strategic actions to fortify their compliance posture:

* **Conduct an Urgent Gap Analysis:** REs, particularly those in long-regulated sectors, must immediately conduct a thorough gap analysis of their existing compliance programs against the new requirements outlined in Section 6. This includes updating systems and procedures for beneficial ownership discrepancy reporting, integrating sanctions evasion into STR protocols, and understanding the implications of the new cash restrictions. For newly regulated entities, this analysis is the foundational step in building a compliant program from the ground up.
* **Re-evaluate and Fortify the Risk Assessment:** The Risk-Based Approach is the element most frequently cited in FINTRAC enforcement actions. The RBA cannot be a static document. It must be a living assessment, regularly updated to reflect new and evolving risks, including those arising from the formal integration of sanctions, the adoption of new technologies, and changes in the RE's business model or client base. The methodology and conclusions of the risk assessment must be meticulously documented and defensible under regulatory scrutiny.
* **Invest in Technology and Training:** In this complex environment, manual compliance processes are increasingly inadequate and prone to error. REs should strategically invest in technology solutions for automated transaction monitoring, real-time sanctions and PEP screening, and digital identity verification. This investment must be paired with a commitment to continuous and sophisticated training that moves beyond basic rules to encompass new typologies, evolving risks, and the critical exercise of judgment required for STR decision-making.
* **Embrace Proactive Engagement and Self-Correction:** REs should not wait for a FINTRAC examination to discover their own weaknesses. The mandatory two-year effectiveness review should be treated as a rigorous, independent audit designed to challenge the program's assumptions and identify failures. If significant issues are discovered, the RE should consider a voluntary self-declaration of non-compliance to FINTRAC. While not a shield from penalties, proactive identification and remediation of issues can be a powerful mitigating factor and demonstrates a positive compliance culture.

### 7.2 Future Outlook: The Road to the FATF Evaluation and Beyond

The current pace of change is unlikely to slow in the near future. The entire regime is being reshaped in anticipation of the FATF mutual evaluation, and the results of that high-stakes review will almost certainly dictate the next wave of legislative and regulatory action.

* **Anticipating Post-FATF Adjustments:** REs should expect that any deficiencies identified by the FATF in its evaluation of Canada's regime will be addressed by the government with further legislative amendments. The period following the release of the FATF report will likely be one of continued regulatory flux.
* **The Rise of Public-Private Partnerships:** The introduction of private-to-private information sharing is a clear signal of a move towards greater collaboration. This trend is likely to continue, potentially evolving into more formalized public-private partnerships and information-sharing mechanisms between government agencies and private sector coalitions to target specific financial crime threats.
* **The Digital Frontier:** The regulatory framework will continue to race to keep up with financial innovation. The evolution of virtual currencies, the emergence of decentralized finance (DeFi), and the increasing use of artificial intelligence in both perpetrating and detecting financial crime will be major drivers of future regulatory development.

### Concluding Analysis

The transformation of Canada's AML/ATF regime reflects a global shift towards a more aggressive and integrated approach to combating financial crime. For businesses operating in Canada, the message from legislators and regulators is unequivocal: compliance is not optional, and the consequences of failure are severe. In this dynamic and high-stakes environment, a robust AML/ATF compliance program is not a cost center to be minimized, but rather a critical strategic function. It is a fundamental component of corporate governance, a prerequisite for sound risk management, and an unavoidable and ongoing commitment for any organization wishing to maintain its license to operate within the Canadian financial system.

#### Works cited

1. Committee Report No. 24 - FINA (42-1) - House of Commons of Canada, https://www.ourcommons.ca/documentviewer/en/42-1/FINA/report-24/page-21 2. What Is FINTRAC PCMLTFA? - AuthenticID, https://www.authenticid.com/glossary/fintrac-pcmltfa/ 3. Proceeds of Crime (Money Laundering) and Terrorist Financing Act - Laws.justice.gc.ca, https://lois-laws.justice.gc.ca/eng/acts/p-24.501/FullText.html 4. Basic Search - Laws.justice.gc.ca, https://www.laws-lois.justice.gc.ca/Search/Search.aspx?&h1dd3n1d=0KDP456CW66U-39&ddC0nt3ntTyp3=Statutes&h1dd3nPag3Num=2&txtT1tl3=%22Proceeds+of+Crime+(Money+Laundering)+and+Terrorist+Financing+Act%22&txtS3archA11=terrorism&h1ts0n1y=0 5. FINTRAC's act and regulations - canafe - Canada.ca, https://fintrac-canafe.canada.ca/act-loi/1-eng 6. Obligations and guidance - canafe - Canada.ca, https://fintrac-canafe.canada.ca/guidance-directives/guidance-directives-eng 7. Upcoming Changes to Canada's Anti-Money Laundering Regime ..., https://mcmillan.ca/insights/publications/upcoming-changes-to-canadas-anti-money-laundering-regime-c2it-that-your-business-is-compliant/ 8. Mandate - canafe - Canada.ca, https://fintrac-canafe.canada.ca/fintrac-canafe/1-eng 9. Criminal Code ( RSC , 1985, c. C-46) - Laws.justice.gc.ca, https://laws-lois.justice.gc.ca/eng/acts/C-46/section-462.31.html 10. www.dlapiper.com, https://www.dlapiper.com/en/insights/publications/2025/03/fintrac-updates-guidance-on-reporting-terrorist-and-sanctioned-property 11. Reporting listed person or entity property to FINTRAC - canafe - Canada.ca, https://fintrac-canafe.canada.ca/guidance-directives/transaction-operation/Guide5/5-eng 12. Reporting suspicious transactions to FINTRAC - canafe - Canada.ca, https://fintrac-canafe.canada.ca/guidance-directives/transaction-operation/str-dod/str-dod-eng 13. Video 3 – What to consider when submitting a suspicious transaction report - canafe, https://fintrac-canafe.canada.ca/training-formation/str-dod/video3-eng 14. Financial crime and sanctions law – 2024 in review and looking ahead | Canada, https://www.nortonrosefulbright.com/en-ca/knowledge/publications/2ac8a9da/financial-crime-and-sanctions-law-2024-in-review-and-looking-ahead 15. Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) - Westlaw, https://content.next.westlaw.com/practical-law/document/I188aad6ff92311e498db8b09b4f043e0/Proceeds-of-Crime-Money-Laundering-and-Terrorist-Financing-Act-PCMLTFA?viewType=FullText&transitionType=Default&contextData=(sc.Default) 16. What you need to know about FINTRAC - QuickBooks - Intuit, https://quickbooks.intuit.com/learn-support/en-ca/help-article/sole-proprietorship/fintrac-articles-incorporation/L9CRoHCMi\_CA\_en\_CA 17. An Overview of the PCMLTFA - Alessa, https://alessa.com/blog/overview-of-the-pcmltfa/ 18. FINTRAC: How Canada's Financial Regulator Works - Investopedia, https://www.investopedia.com/terms/f/fintrac.asp 19. Learn about how OSFI and FINTRAC work together, https://www.osfi-bsif.gc.ca/en/risks/learn-about-osfi-fintrac-work-together 20. Guidance and resources for businesses (reporting entities) - canafe - Canada.ca, https://fintrac-canafe.canada.ca/guidance-directives/1-eng 21. PCMLTFA Compliance in Canada - Arctic Intelligence, https://arctic-intelligence.com/countries/compliance-canada 22. mastering compliance - Gov.bc.ca, 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 23. Financial Transactions and Reports Analysis Centre of Canada, https://www.canada.ca/en/financial-transactions-reports-analysis.html 24. Audit of the Financial Transactions and Reports Analysis Centre of Canada, https://www.priv.gc.ca/media/1138/ar-vr\_fintrac\_2013\_e.pdf 25. FINTRAC - Info Source, https://fintrac-canafe.canada.ca/atip-aiprp/infosource-eng 26. FINTRAC to publicly name violators of anti-money laundering rules - Norton Rose Fulbright, https://www.nortonrosefulbright.com/en-gb/knowledge/publications/c6b03a28/fintrac-to-publicly-name-violators-of-anti-money-laundering-rules 27. The Proceeds of Crime (Money Laundering) and Terrorist Financing Act: What you need to know, https://publications.gc.ca/collections/collection\_2017/canafe-fintrac/FD4-9-2012-eng.pdf 28. Federal Court clarifies approach to administrative monetary penalties for failing to report suspicious transactions | DLA Piper, https://www.dlapiper.com/en/insights/publications/2025/05/federal-court-clarifies-approach-to-administrative-monetary-penalties 29. Access to Information and Privacy Protection at FINTRAC - canafe, https://fintrac-canafe.canada.ca/atip-aiprp/privacy-privee-eng 30. Financial Entities - canafe - Canada.ca, https://fintrac-canafe.canada.ca/re-ed/fin-eng 31. Anti-money laundering compliance (Fintrac) - Canadian Home ..., https://www.chba.ca/anti-money-laundering-compliance-fintrac/ 32. Video – Mortgage Sector: Compliance program requirements - canafe - Canada.ca, https://fintrac-canafe.canada.ca/training-formation/mortgage-hypotheque/video-eng 33. Canadian Anti-Money Laundering Law: What you need to know about compliance program requirements - Osler, Hoskin & Harcourt LLP, https://www.osler.com/en/insights/blogs/risk/canadian-anti-money-laundering-law-what-you-need/ 34. Breaking down FINTRAC's Anti-Money Laundering (AML) compliance crackdown - MNP, https://www.mnp.ca/en/insights/directory/business-need-know-fintrac-anti-money-laundering-compliance 35. FINTRAC Amends PCMLTFA - More AML Requirements for Reporting Entities - Shufti Pro, https://shuftipro.com/blog/fintrac-amends-pcmltfa-more-aml-requirements-for-reporting-entities/ 36. Administrative monetary penalties policy - canafe - Canada.ca, https://fintrac-canafe.canada.ca/pen/2-eng 37. FINTRAC Fines & Penalties for Non-Compliance - Renno & co, https://www.rennoco.com/blog/fintrac-fines-for-msb-non-compliance 38. Proceeds of Crime (Money Laundering) and Terrorist Financing Administrative Monetary Penalties Regulations ( SOR /2007-292) - Laws.justice.gc.ca, https://laws-lois.justice.gc.ca/eng/regulations/SOR-2007-292/FullText.html 39. FINTRAC Administrative Monetary Penalties: Addressing the Centre's Tool for Compliance - Tax & Trade Blog - Millar Kreklewetz LLP, https://www.taxandtradelaw.com/Tax-Trade-Blog/fintrac-administrative-monetary-penalties-addressing-the-centre-s-tool-for-compliance.html 40. Canada Accelerates Amendments to Its Anti-Money Laundering and ..., https://www.blakes.com/insights/canada-accelerates-amendments-to-its-anti-money-laundering-and-anti-terrorist-financing-regime/ 41. Final accelerated changes to Canada's AML/ATF regime released ..., https://gowlingwlg.com/en/insights-resources/articles/2025/changes-to-canada-s-aml-atf-regime 42. Lessors and financiers take note — New Canadian AML regulations in force | DLA Piper, https://www.dlapiper.com/en/insights/publications/2025/04/new-canadian-aml-regulations-in-force 43. Understanding the Recent Amendments to Proceeds of Crime ..., https://www.eservicecorp.ca/amendments-to-aml-regulations/ 44. Federal government fast-tracks changes to Canada's AML regime, https://www.osler.com/en/insights/updates/federal-government-fast-tracks-changes-canadas-aml-regime/ 45. Modernization and upcoming changes impacting reporting entities - canafe - Canada.ca, https://fintrac-canafe.canada.ca/businesses-entreprises/changes-changements-eng