Updated Assessment of Inherent Risks of Money Laundering and Terrorist Financing Summary

**Executive Summary**

The report provides a comprehensive update to Canada's 2015 national assessment of inherent money laundering (ML) and terrorist financing (TF) risks, reflecting analysis up to December 2020.1 Its purpose is to identify and understand these risks

*before* the application of any mitigating controls, serving as a critical tool for over 24,000 regulated entities to inform their own risk-based compliance programs.1

* **Methodology:** The assessment evaluates threats and inherent vulnerabilities across Canada's economy, key sectors, and financial products. By matching threats with vulnerabilities, the report constructs risk scenarios to identify the areas most exposed to ML/TF.1
* **Key Findings on ML Threats:** The threat of money laundering is rated "very high" for illicit drug trafficking, various types of fraud (including commercial trade, capital markets, and mortgage fraud), illegal gambling, corruption, and third-party money laundering. Transnational organized crime groups (OCGs) and professional money launderers are identified as the primary threat actors.1
* **Key Findings on TF Threats:** While networks suspected of raising funds for terrorist groups operate in Canada, the overall TF threat is considered less pronounced than in other parts of the world, partly due to the strength of Canada's existing anti-terrorist financing regime.1
* **Key Findings on Vulnerabilities:** Several sectors are rated as having "very high" vulnerability to ML/TF, including domestic banks, corporations (particularly private ones), certain money services businesses (MSBs), and express trusts. These vulnerabilities stem from high accessibility, large transaction volumes, exposure to high-risk clients and jurisdictions, and opportunities for anonymity.1

### **Canada's Risk Mitigation Framework (AML/ATF Regime)**

Canada's Anti-Money Laundering and Anti-Terrorist Financing (AML/ATF) Regime is a coordinated framework operated by 13 federal partners, including the Department of Finance, FINTRAC, OSFI, and the RCMP. It is built on three interdependent pillars 1:

1. **Policy and Coordination:** Led by Finance Canada, this pillar establishes the legal framework, primarily through the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA). The PCMLTFA mandates that reporting entities (like banks, real estate agents, and casinos) identify clients, keep records, report specific transactions (e.g., suspicious transactions, large cash transactions), and implement a risk-based compliance program. This pillar also involves domestic and international coordination with bodies like the Financial Action Task Force (FATF).1
2. **Prevention and Detection:** This pillar focuses on preventing illicit funds from entering the financial system. Reporting entities are the frontline defense, supervised by regulators like FINTRAC and OSFI. FINTRAC, as Canada's financial intelligence unit, collects and analyzes financial transaction reports, disseminating intelligence to law enforcement and national security agencies. In 2019-20, FINTRAC made 2,057 such disclosures.1
3. **Disruption:** This pillar involves the investigation and prosecution of ML/TF offenses by law enforcement agencies, supported by FINTRAC's intelligence. It includes the restraint and confiscation of the proceeds of crime and a robust process for listing terrorist entities to freeze their assets.1

### **Methodology for Risk Assessment**

The assessment defines risk as a function of three components: threats, inherent vulnerabilities, and consequences.1

* **Threats:** A person or group with the intent to launder money or finance terrorism. ML and TF threats are assessed separately.
  + **ML Threat Criteria:** Rated based on sophistication, capability, scope, and the magnitude of proceeds of crime generated.1
  + **TF Threat Criteria:** Rated based on sophistication, capability, scope of fundraising, estimated value of fundraising, diversification of methods, and the suspected use of funds against Canadian interests.1
* **Inherent Vulnerabilities:** Properties within a sector or product that can be exploited by threat actors. Vulnerabilities are assessed against criteria including the sector's inherent characteristics (size, complexity), the nature of its products and services, client relationships, geographic reach, and the anonymity afforded by its delivery channels.1
* **Consequences:** The harm caused by ML/TF to society, the economy, and government, including increased crime, economic distortions, and erosion of public institutions.1

### **Assessment of Money Laundering (ML) Threats**

The assessment identifies a broad range of profit-oriented crime in Canada generating billions in proceeds annually.

* **Key Threat Actors:** The most significant threats are transnational OCGs and the professional money launderers they employ. These groups use sophisticated, complex global networks to launder proceeds from crimes like drug trafficking. Other key actors include nominees, money mules, and criminalized professionals (e.g., lawyers, accountants) who facilitate illicit schemes.1
* **Very High-Rated ML Threats:**
  + **Illicit Drug Trafficking:** Remains the largest criminal market in Canada.1
  + **Fraud:** Includes capital markets fraud, commercial (trade) fraud, mass marketing fraud, and mortgage fraud.1
  + **Illegal Gambling:** This threat was upgraded to "Very High" due to its high profitability for organized crime and an observed increase in underground activity during COVID-19 lockdowns.1
  + **Corruption, Collusion, and Bribery:** A significant threat, particularly concerning the illegal acquisition of high-value public contracts.1
  + **Third-Party Money Laundering:** Professional launderers, often the masterminds behind large-scale schemes, pose the greatest threat in this category.1

### **Assessment of Terrorist Financing (TF) Threats**

Terrorism remains a leading threat to Canada's national security.

* **Overall Threat:** While networks exist in Canada to raise and transmit funds for various terrorist groups, the overall TF threat is considered less pronounced than in other regions of the world with weaker AML/ATF regimes.1
* **Methods:** Financing methods include the use of MSBs, banks, registered charities, bulk cash smuggling, and the procurement and sale of high-value goods (e.g., electronics) in jurisdictions of concern.1
* **Emerging Risk—Ideologically Motivated Violent Extremism (IMVE):** This is a key emerging threat. IMVE financing is often characterized by low-sophistication methods. Lone actors typically use personal funds for small-scale purchases like weapons, while organized groups may use crowdfunding, merchandise sales, and membership fees to fund their activities. There is also evidence of individuals in Canada funding international IMVE networks through small, recurring international transfers.1

### **Assessment of Inherent Vulnerabilities**

The assessment rated 33 economic sectors and financial products, finding a significant number to be inherently vulnerable to ML/TF.

* **Very High Vulnerability Sectors:**
  + **Domestic Banks:** Vulnerable due to their large size, high transaction volumes, international reach, and diverse, high-risk client base.1
  + **Corporations and Express Trusts:** Highly vulnerable because they can be used to conceal beneficial ownership through complex legal structures, making it difficult to trace illicit funds.1
  + **Certain Money Services Businesses (MSBs):** Both retail multi-service MSBs and alternative remittance MSBs (including virtual currency exchangers) are rated very high due to their accessibility, high volume of transactional business, and potential for anonymity.1
* **High Vulnerability Sectors:** This category includes 18 sectors and products, notably:
  + **Real Estate:** Vulnerable to price manipulation, the use of nominees, and the obscuring of fund sources, with risks amplified by rapid price increases in some regions.1
  + **Casinos:** Highly vulnerable due to being cash-intensive and highly transactional. The "Vancouver Model" is a specific high-risk scenario involving casinos, underground banking, and real estate to launder funds from China.1
  + **Securities Dealers:** Vulnerable due to high-value transactions, international reach, and products that can be used in the layering stage of money laundering.1
  + **Legal Professionals:** Vulnerable as their services (e.g., creating trusts and corporations, managing trust accounts) can be wittingly or unwittingly exploited to add a layer of legitimacy to illicit schemes.1

### **Evolution of the Risk Landscape Since 2015**

The risk landscape in Canada is dynamic and has evolved since the last assessment.

* **Changing Threats:** The threat levels for illegal gambling, tax evasion, and wildlife trafficking have increased. New criminal typologies have emerged, particularly related to the fentanyl trade, online fraud schemes, and the use of virtual assets.1
* **New Vulnerabilities Assessed:** The scope of the assessment was broadened to include sectors like armored car companies, unregulated mortgage lenders, and import/export companies, recognizing their inherent vulnerabilities.1
* **Impact of Technology and Events:** The rapid growth of virtual assets presents new challenges. The COVID-19 pandemic accelerated the shift to digital finance, which, while demonstrating the sector's adaptability, also created new opportunities for criminals to exploit online schemes and digital payment platforms.1