Deloitte.


# Combatting money laundering in the fight against financial crime

November 2019

Combatting money laundering in the fight against financial crime

# Introduction

Financial crime is a global, US$2.1-trillion-a-year issue[1], and as globalization makes overseas markets more accessible, Canada's share of this underground economy is becoming more apparent. As has been widely reported, Canada, and British Columbia, have become a haven for illicit funds entering the legitimate economy by way of financial crime[2]. This has serious implications for Canada's reputation, for our economy, and for our society as a whole.

Financial crime involves making money illegally from transnational organized crime, tax evasion, corruption, securities fraud, drug and human trafficking, and embezzlement. Money laundering is the act, or attempted act, of making the proceeds of a crime appear legitimate. Money laundering itself cannot occur in a vacuum—it always involves the commission of a crime, such as those mentioned above, which is called a ***predicate offence***.

Because money laundering can't occur in isolation, it can't be combatted in isolation either. Siloed efforts may result in losing sight of both the intelligence gathered through the investigation of the predicate offences and the risks associated with those offences. An entity that has traditionally tackled financial crime by setting up separate groups for different types of financial crime may inadvertently undermine its own risk-mitigation strategy.

To effectively detect, manage, and curb financial crime, stakeholders need to implement more cohesive and integrated financial-crime programs.




# Financial crime reduction as a public safety issue

Understanding the synergies between money laundering and its predicate offence(s) is essential for effectively identifying, investigating, enforcing, and mitigating these crimes with the necessary resources, policies, processes, and infrastructure at the federal, provincial, and private-sector levels.

Financial crime is organized and transnational, meaning both the criminal acts and the illicit funds generated cross provincial, territorial, and international boundaries. As a result, combatting it must involve multi-jurisdictional, public-private cooperation and coordination. This complex challenge requires continuous dialogue between governmental and regulatory bodies, reporting entities, industry representatives, and global and local independent watchdogs in order to develop mechanisms for intelligence-gathering and data-sharing. Money laundering can occur a great distance from where the predicate offence took place. Professional money launderers are well aware that they can only be convicted of money laundering in Canada if they are linked to a predicate offence, so they take great care to structure their businesses in a way that insulates one from the other. Mexican cartels and Iranian and Chinese organized crime, for example, have come to Greater Vancouver to wash billions of dollars in crime proceeds that originated in other countries[3]. So, to fight financial crime in Canada, it's critical that we implement measures to identify, investigate, and successfully prosecute the laundering of dirty money.

Under increasing pressure to address financial crime, both public and private-sector leaders are looking to innovate and take a more holistic approach.

Recognizing the connection between money laundering and its predicate offences, and integrating data more effectively across jurisdictions and organizations, will go a long way to improving public policymaking and mitigating the impacts of financial crime.

By disrupting domestic and transnational organized crime networks, governments and businesses can help ensure public safety and quality of life. There are both direct and indirect benefits of financial-crime reduction as a public policy, including:

- Tackling the opioid epidemic
- Reducing gang violence
- Improving housing affordability
- Decreasing poverty
- Increasing income equality

These efforts will require cooperation across all levels of government, justice and security, and the private sector. Developing policy and implementing it will take many years, but day-to-day operations cannot be neglected. Governments should, therefore, start by establishing a project management office to:

- Assess the current state of its financial crime framework, and identify pain points
- Develop a future-state vision
- Determine what funding is required to build the future-state vision, and where it will come from
- Create a roadmap to reach the future-state vision and identify quick wins, prioritizing immediate activities to disrupt illicit activity
- Begin a cohesive, phased, and iterative approach to enhance the financial-crime-fighting framework, including:
  - Using change management to start fostering a collaborative, innovative, risk-based culture
  - Implementing a rigorous governance and oversight framework, focusing on clear roles and responsibilities, accountability, reporting, and communication
  - Updating, amending, or drafting legislation to strengthen current policy
  - Exploring the convergence of various financial-crime functions to support information sharing, investigation, and enforcement
  - Creating independent oversight bodies in high-risk industries
  - Developing a data strategy and building the required IT infrastructure
  - Independently assessing the effectiveness of the framework once it is implemented

We recognize that none of these activities is entirely within the control of one level of government, or even one ministry.

Next, we address additional considerations that will need to be integrated into an effective financial-crime-fighting framework for British Columbia.

## Governance

To ensure alignment, efficiency, and transparency, the framework should be guided by a governance model that defines the mechanisms and interaction points across the various ministries, agencies, and associated entities.

There are three crucial components to a successful governance model:

### 1 Establish one primary public supervisory body or committee, supported by clear terms of reference (TOR).

For example, with the creation of a new independent crown agency, the BC Financial Services Authority (BCFSA), to regulate credit unions, insurance and trust companies, pensions, and mortgage brokers, the province has built a critical foundation for the effective, holistic supervision of financial crime, and money laundering in particular. The dedicated Office of the Superintendent of Real Estate (OSRE) and the Real Estate Council of British Columbia (RECBC), to name a couple, also form part of the foundation of this governance structure.

Relevant stakeholder agencies and Ministries need to operate under one common framework which allows for collaboration, especially as it relates to data sharing, to be fully effective in combatting money laundering. As an example, this could be achieved by, inter alia, the formation of one primary supervisory authority or committee to oversee the overall coordination of all the stakeholders, resources, and priorities, while maintaining independence of each institution. This will pave the way for effective planning and implementation, with a clear view of priorities, approach, and roles and responsibilities.

Critical success factors to be effective is the assignment of authority to this primary supervisory body or the governing committee, including, for example:

- Access to current data in an appropriate format in order to support analysis and investigation
- Requiring timely and complete reporting on regulated entities
- Conducting assessments of the accuracy and validity of reporting, and imposing penalties or enforcement actions on non-compliant organizations

### 2 Develop an integrated public-private partnership model.

A public-private partnership approach to information- and data-sharing will ensure that participants can meet regulatory standards while remaining competitive in the global economy. This model has proven effective in other countries, as well as within the financial services industry, supporting balanced, insight-driven decision-making in a complex environment. This approach will also streamline operations across government entities, benefitting BC and Canada more broadly.

Within the overall governance structure, this public-private partnership model should be highly formalized, making sure that all parties have defined accountabilities, roles, and responsibilities, and that they align their activities to a defined strategy. Developing a business case for participants that focuses not only on the benefits of reducing risks, but also on the economic benefits of improving BC's competitive advantages may accelerate the process.



Combatting money laundering in the fight against financial crime

### 3 Focus on independence, quality assurance, performance measurement, and transparency.

The governance framework can optimize independence and quality by applying the three lines of defense model[4] to regulated bodies, focusing on oversight, accountability, and enforcement. This will also create credibility in interactions with government stakeholders, industry, and the broader public.

The framework should include measurable performance and risk indicators, including policing and enforcement statistics, compliance data, and transactional information, because tracking the progress of these financial-crime-reduction efforts will be a significant factor in the program's success. It may also lead to increased enforcement and successful prosecutions. Continuous tracking will allow stakeholders to analyze trends, highlight and manage emerging risks, and refocus resources appropriately to continue making progress as conditions evolve.

Finally, a comprehensive, appropriately transparent communication strategy will keep the public informed of the government's priorities and progress in the fight against money laundering and organized crime. The public's reaction could also give stakeholders further data to guide any changes required to plan for this multi-year initiative.

## Privacy

Privacy legislation varies from province to province, and has often been seen as a barrier to information-sharing and analysis. However, organizations in Canada have found effective approaches that improve analytical capabilities while maintaining individuals' privacy rights. Any financial-crime-fighting initiative should consider a privacy by design approach, in which privacy risks are identified and appropriate privacy controls are built in from the beginning[5]. Furthermore, privacy regulators should be engaged early in the process to identify principles for data-sharing and to monitor these practices to confirm ongoing alignment with legislation and with citizens' expectations.

Recognizing that legislative changes to enable data integration take time, a practical first step to data-sharing might involve anonymization solutions. These allow analysts to work with data while protecting the identity of the associated individuals. Specific individuals of interest can then be identified when certain thresholds are met that justify direct engagement with them.

## Cybersecurity

Increased data-sharing heightens the risk of data concentration and data breach. In an environment where multiple sensitive data sets are integrated for analysis, a risk-based approach to security and information protection is necessary. The specific technical approach to cybersecurity will depend on how and where data is collected, integrated, and analyzed.

Some organizations have created dedicated physical data centres where large volumes of data are aggregated. Others have created virtual data integration environments that are accessed through secure, remote channels, while other entities have taken a hybrid approach. Whichever model is used, the security approach must be based on a robust analysis of threats and risks. Effective security controls must be augmented by continuous monitoring, as well as ongoing enhancements, to address new threats and risks as they arise.

## Data analytics

Continual advances in technology are changing our ability to efficiently detect the indicators of financial crime. Ongoing monitoring for unusual or suspicious activity has traditionally been rules-based, and has typically looked at transactions in isolation. The rule sets themselves are defined based on static inputs, with little consideration for how different thresholds might affect red-flag alerts and false-positive results. Consequently, the majority of transaction-monitoring system alerts generate a tiny percentage of actual cases, and even fewer reports to regulators. Large institutions and enforcement agencies are drowning in an ever-increasing sea of alerts, creating a large backlog that requires subject-matter expertise to get through but is seen to provide limited value.

Many organizations are now turning to a more sophisticated approach to monitoring transactions and activity that combines humans with machine learning. Because of regulatory expectations in numerous jurisdictions, including the United States, industry is moving away from rules-based systems focused on defined risk scenarios toward a model-based artificial intelligence (AI) approach that detects suspicious behaviours across a wide range of data sources. Applying machine learning in certain contexts can massively accelerate the development of subject-matter expertise while "human" capacity is increased.

Good data can add significant value not only to public policy decisions, but to investigations and enforcement as well. Unfortunately, data is not always collected with these disparate purposes in mind. As a result, data sets are often poorly structured and/or incomplete, making them difficult to manipulate using traditional analysis techniques. Modern, deep-learning models can be used to cleanse and mine unstructured data for insights, generating structured data for other uses in the process. Going well beyond keyword searches, today's machines can understand the meaning of text (i.e., natural language) and can be used to comb through social media feeds or news articles to identify information about suspicious actors and enrich existing datasets.

Dataset re-use and interoperability can be improved by thinking about data collection and analysis as an end-to-end solution. What data is collected, how, and by whom all have implications on its quality and ongoing usability. Adapting the method of collection (e.g., using e-forms, and using dropdowns rather than free-form text fields) and ensuring the right fields are included will improve data quality and reduce the cost of transforming data for intelligence purposes.

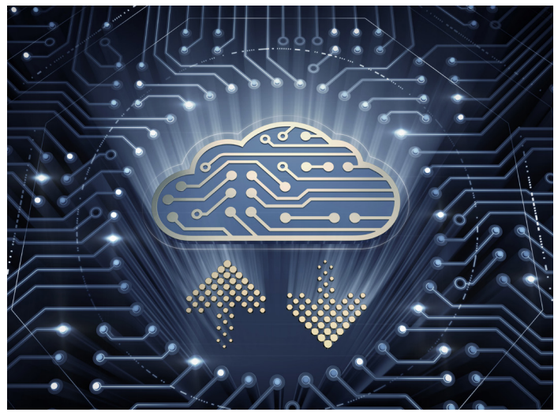
## Technology architecture & implementation

Technology and automation solutions can accelerate data collection, aggregation, analysis, and investigation. Deriving value from a financial-crime-focused technology implementation requires a centralized, scalable, systematic, and repeatable methodology with the objectives of:

- Amalgamating information across disparate sources to provide a complete view of a transaction or subject of interest and its connected counterparties
- Layering in open-source and subscription-based information to enrich information, fill gaps, and return true matches with a higher degree of confidence
- Identifying networks of relationships to review transactions and spot high-risk indicators such as money laundering, non-compliance with regulations, and ineffective supervision
- Accessing a unified intelligence portal that allows investigators to perform consistent analysis and maintain required standards in reporting

The underlying technology architecture needs to be able to handle large volumes of transactions (i.e., Big Data) and integrate existing client systems and other third-party tools. A clear Big Data or data-lake strategy, combining supervised and unsupervised AI, is essential for successfully using artificial intelligence to identify unusual patterns and effectively combat financial crimes.

The infrastructure hosting the centralized information, whether on-premise or in the cloud, will require continuous management and investment to make sure the data is current, the modelling is effective, and the reporting and/or intelligence output is as valuable as possible.





Combatting money laundering in the fight against financial crime

## Policy and regulation

Financial crime legislation and regulation in Canada is primarily federal and focuses on anti–money laundering (AML) and anti-terrorist funding (ATF). Since financial crime does not respect political boundaries, a comprehensive federal regulatory framework is certainly required. However, the lack of provincial integration into the federal regulatory framework has left the provinces accountable for financial crime within their borders without having the necessary powers to deal with it.

Although it is not completely within a provincial government's remit to strengthen its financial crime-mitigation framework, there are actions provinces can take that would have a significant impact on their money-laundering risk. The BC government, for one, has already taken some steps, introducing legislation to form a beneficial ownership registry for real estate and requiring more due diligence on casino players' sources of funds on transactions above a certain threshold.

As for federal regulation, a particular shortcoming of Canada's commitment to AML has been that certain real estate-related businesses have not been covered as reporting entities under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA). These include legal professionals, unregulated mortgage lenders, mortgage insurers, land registries, title insurance companies, promoters, and re-developers. It has also been a challenge for AML officers to get accurate, up-to-date data on their clients, given the lack of verified information in the public domain.

The federal government has now committed to expanding legislation to cover more high-risk industries, and to more strictly enforcing AML/ATF policies. It is also working to improve information sharing between the private sector, provincial agencies, federal law enforcement, and financial regulators.

The overarching implication for reporting entities is that they will be expected to provide more information in shorter time frames with greater accuracy. It will no longer be enough to just comply with a set of rules. Instead, they will have to supply actionable financial intelligence that will help detect money laundering and terrorist financing in Canada.

Government and regulators will need to coordinate closely with reporting entities to help them meet these requirements and ensure that their reporting supports investigation and enforcement activities.

# Quick wins to disrupt illicit activity

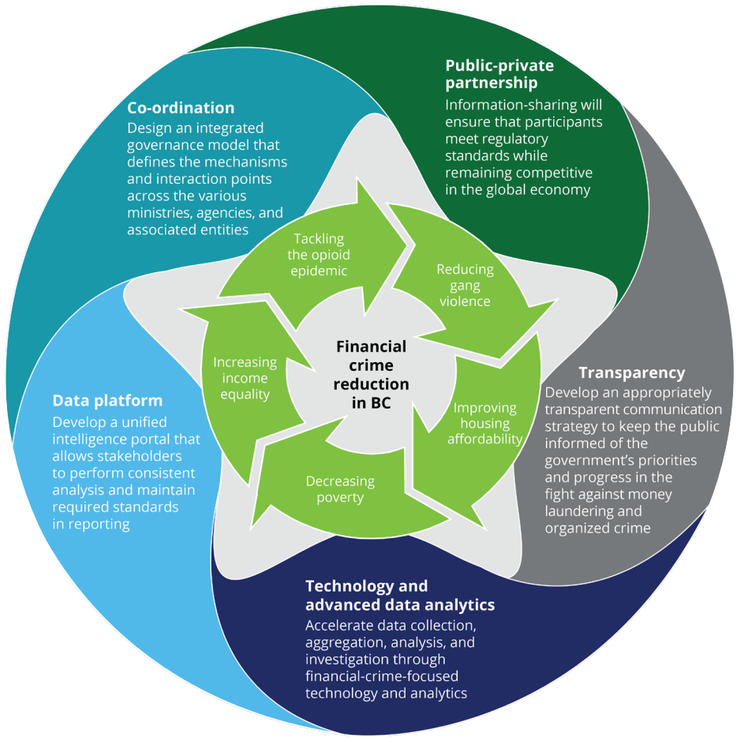
Several measures should be implemented federally, provincially, and locally to strengthen the AML regime, and promote public safety, including several short-term actions that will help us better understand and mitigate financial crime risks. These will not only help prevent the proceeds of crime from entering Canada's financial system, but also support public safety initiatives.

## Strengthening the AML framework

The Financial Action Task Force (FATF) delivered a Mutual Evaluation Report on Canada in 2016, assessing its compliance and effectiveness in implementing the 40 FATF recommendations to counter money laundering. The report found Canada has significantly lagged behind in its commitment to compliance.

Apart from the federal government's activities to respond to these findings, the BC government has developed its own priorities for enhancing public safety, disrupting organized crime and identifying unexplained wealth, as one example.

This is a multi-faceted goal, which will require input, alignment, and cooperation between various provincial ministries, agencies, and crown corporations; the federal government; and regulatory bodies. The next step is for a provincial government to shape its vision and create a collaborative roadmap to success. This map should include underlying strategies and plans for each responsible ministry or agency, ensuring their activities are aligned where needed. Although the BC government can only control activities within the province, its plans can help facilitate the changes in other provinces and at the federal level.








## Beneficial-ownership transparency

Canada is developing an unwelcome reputation as a jurisdiction of international financial secrecy. As the country attempts to tackle financial crime, the limelight is on BC's beneficial-ownership registry and its Land Owner Transparency Act (the Transparency Act). This is a one-of-a-kind attempt to combat money laundering and tax fraud by increasing transparency and putting a stop to the hidden ownership of land. Once the registry goes online in 2020 (estimated), numbered companies, offshore trusts, and corporations will find it more difficult to remain anonymous, as the names of beneficial owners, partners, and controlling shareholders will be made available to the public.

In 2016, the United Kingdom created its own public register of the beneficial owners of companies, called the register of People with Significant Control (PSC). Canada can learn some critical lessons from the UK experience. The PSC is an open registry that makes all data publicly accessible and makes it possible to analyze the data as a whole rather than look at each company's records individually. The UK has successfully addressed questions about data security and privacy in the PSC, but is still struggling with accuracy due to a lack of verification of information collected. For instance, it allows individuals to seek exemptions to publishing certain data, if they can prove that releasing it would pose a serious risk of violence due to the nature of their company's operations.

BC's Transparency Act does not currently specify the format in which data would be made available to the public or the fees for accessing it. Interesting to note that the United Kingdom recently shifted from a paywall to publicly available.

## Criminal and civil enforcement

Overall, Canada has a poor record of successfully investigating and prosecuting financial crime, particularly money laundering. This is partly because the legislation requires that the predicate offence be proven to prosecute money-laundering charges, unlike in the European Union and certain other jurisdictions. So Canadian law enforcement needs both the resources and the mechanisms to pursue the transnational organized crime groups that use Canada to either park or launder the proceeds of their crimes.

Yet, enforcement agencies in Canada simply don't have enough skilled resources, information, or data to successfully investigate these crimes. A federal intelligence unit, which incorporates data from governmental and regulatory sources across the country and runs it through advanced analytical models will create useful intelligence. We need to provide sufficient funding and infrastructure to skilled, experienced resources—who understand the link between predicate offences and the laundering of their financial proceeds—to investigate and prosecute these offences in a timely manner.

The Ontario appeal court cases, R. v. Phu Nhi (John) Trac[6] and Project Roadmaster[7] provide good examples of effective collaboration in multi-agency investigation. These cases involved the use of nominees and numbered and shell companies to launder the proceeds of illicit funds through numerous bank accounts, real estate transactions, and luxury-goods purchases. In both of these cases, law enforcement traced the origins of the laundered funds through various geographies, bank accounts, and companies, taking a holistic view of all aspects of complex illicit conduct and using specialized knowledge and skills relating to specific offences. The result in both cases was a successful investigation and prosecution of predicate offences and money-laundering charges.

Regulators are responsible for mitigating financial crime risk by setting industry standards, monitoring compliance of reporting entities, and administering penalties or sanctions as needed. Reporting entities have a contribution to make as well, by refusing to accept a criminal person or entity as a client, supporting law enforcement with their investigations, filing suspicious transaction reports, etc. Effective data-sharing practices between regulators and reporting entities will allow for better understanding of financial crime trends, enable enhanced policy development and decision-making, and ensure there are no undue burdens or expectations on participants in a highly competitive market.

Transparency International Canada, in its March 2019 report ***Why Criminals Love Real Estate (And How to Fix It)***, noted that enforcement of the law in the real estate sector is poor and that criminal sanctions for money-laundering offences are disappointingly rare. Despite having the statutory authority to sanction entities that fail to comply with its obligations, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) has not issued any penalties since 2016. The report cited under-resourced law enforcement and a shortage of specialist financial-crime investigators as loopholes in Canada's AML framework, and although civil forfeiture tools exist for law enforcement agencies, they are underused in the real estate sector. Improving public-private data-sharing and providing more financial-intelligence tools will make law enforcement more effective.



# The future of combatting financial crime

As BC develops a strong, efficient AML ecosystem, the rest of Canada will begin to feel the pressure if it doesn't take similar measures. The proceeds from illicit funds coming into the country will likely continue to find their way into other provinces that don't follow BC's lead.

With regulatory pressure and the increase in sophisticated financial-crime attacks, focusing budgets, resources, and the commitment of financial crime and compliance teams has become the logical next step.

Significant political will is required across every part of the government to make far-reaching changes to policy, oversight, and enforcement, in both the public and private sectors, to alter Canada's reputation as easy prey for criminal activity. This is BC's moment to ensure the ongoing safety of our citizens, stability of our economy, and the strength of our international relations.

# References


[1]Deloitte, “The Future Operating Model of Financial Crime Report,” 2019.

[2]Canada a hotbed for money laundering: Report, Ottawa Citizen, available at https://ottawacitizen.com/news/national/canada-a-hotbed-for-money-laundering-report/wcm/b9d29c2a-e4d6-48c7-9430-6ab9ff654686

Weak rules have made Canada a magnet for money laundering, CBC, available at https://www.cbc.ca/news/business/money-laundering-canada-1.5125078

[3]Bloomberg, "A laundromat for foreign organised crime': Billions in dirty cash from China, Iran, Mexico helped fuel Vancouver housing boom, report finds," South China Morning Post, May 10, 2019. https://www.scmp.com/news/world/united-states-canada/article/3009632/laundromat-foreign-organised-crime-billions-dirty

[4]Three lines of defence: 1) functions that own and manage risk, 2) functions that oversee or specialize in risk management and compliance, 3) functions that provide independent assurance, i.e., internal audit.

[5]Ann Cavoukian, Privacy by Design. The 7 Foundational Principles: Implementation and Mapping of Fair Information Practices. https://iapp.org/media/pdf/resource_center/Privacy%20by%20Design%20-%207%20Foundational%20Principles.pdf

[6]R. v. Trac, 2013 ONCA 246 http://www.ontariocourts.ca/decisions/2013/2013ONCA0246.htm

[7]Niagara Regional Police, 2014 Annual Report, p. 36 https://www.niagarapolice.ca/en/contentresources/resources/whoweare/2014_Annual_Report.pdf


Combatting money laundering in the fight against financial crime

# Contacts


**Peter Dent**
**Partner**
Financial Advisory
416-601-6692
pdent@deloitte.ca



**Christine Ring**
**Partner**
Financial Advisory
416-775-8851
cring@deloitte.ca



**Jamie Ross**
**Partner**
Risk Advisory
250-978-4412
jaross@deloitte.ca



**Andrew Medd**
**Partner**
Consulting
250-978-4436
amedd@deloitte.ca

Deloitte.

Deloitte provides audit & assurance, consulting, financial advisory, risk advisory, tax and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries and territories bringing world-class capabilities, insights and service to address clients' most complex business challenges. To learn more about how Deloitte's approximately 264,000 professionals—9,400 of whom are based in Canada—make an impact that matters, please connect with us on LinkedIn, Twitter or Facebook.