FINANCIAL INDUSTRY FORUM ON ARTIFICIAL INTELLIGENCE II:

A COLLABORATIVE APPROACH TO AI THREATS, OPPORTUNITIES, AND BEST PRACTICES

WORKSHOP 2 - FINANCIAL CRIME

NOVEMBER 2025

GLOBAL RISK INSTITUTE

Financial Transactions and Reports Analysis Centre of Canada
Centre d'analyse des opérations et déclarations financières du Canada

> This forum is vital as it focuses on one of the most pressing and complex challenges we face today...combatting financial crimes in the age of Artificial Intelligence. Now more than ever, we need a strong, well-equipped, and committed network to defeat modern criminal and terrorist networks. We know we can't do this alone. We need a whole-of-ecosystem approach: one that brings together financial institutions, technology providers, regulators, and researchers to build resilient, ethical, and effective AI solutions.
>
> Sarah Paquet, Director and Chief Executive Officer, FINTRAC. October 1, 2025

PREFACE

On October 1, 2025, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) and the Global Risk Institute (GRI) co-sponsored a workshop on Financial Crimes and Artificial Intelligence as part of the Financial Industry Forum on Artificial Intelligence II: A Collaborative Approach to AI Threats, Opportunities, and Best Practices. This second workshop in the FIFAI II process brought together over 60 Canadian and international experts in financial crime and artificial intelligence (AI) from the financial industry and their regulators.

The first workshop, held in May 2025, identified opportunities, risks, and threats related to security and cybersecurity. The report documenting participant perspectives is available here.

The objective of the workshop on Financial Crimes and AI was to:

> Identify AI-driven risks, mitigations and opportunities related to financial crime to learn how AI can help detect and prevent financial crime through smarter, faster, and more adaptive risk management focused on i) fraud and fraud management, ii) anti-money laundering (AML), iii) sanctions compliance and evasion, and iv) insider threats and data integrity.

This effort continues the work started three years ago, when OSFI and GRI initiated a discussion on AI risks and opportunities, hosting the first Financial Industry Forum on Artificial Intelligence (FIFAI I) in 2022 to promote responsible AI use in Canada's financial sector. The resulting report, "A Canadian Perspective on Responsible AI," emphasized the importance of implementing comprehensive risk management strategies to address the specific challenges presented by AI.

There are two remaining workshops in the FIFAI II process: one on Consumer Protection and one on Financial Stability. In addition to the interim reports for each workshop, there will also be a final report which will cover key insights and best practices across all four workshops.

AI presents both opportunities and risks for the financial sector. The sponsors, FINTRAC and GRI, would like to express their sincere gratitude to all workshop participants for their engagement in this collaborative dialogue.

Global Risk Institute

Financial Transactions and
Reports Analysis Centre of Canada
(FINTRAC)

FINANCIAL CRIME – INDUSTRY AND REGULATORY PERSPECTIVES ON RISKS, MITIGATION, AND OPPORTUNITIES

Financial crime, including fraud, money laundering, sanctions evasion, and insider fraud, has grown in scale, scope, and speed over the past decade. The AI revolution has increased these risks and complicated Canada's ability to prevent and defend against these financial crimes.

Workshop perspectives on AI adoption and financial crime

The workshop identified that appropriately targeted AI investment can improve both the effectiveness and efficiency of a financial institution's efforts to fight financial crime. Such AI adoption is now shifting from pilot projects to wider implementation.

When asked about the barriers preventing organizations from adopting AI to enhance financial crime detection, 48% of workshop participants identified cost and resource constraints as the most significant obstacle.

Forum participants also identified "fraud" as the financial crime most likely to increase due to the use of AI over the next two to three years.

Figure 1: Participant questionnaire, October 1, 2025

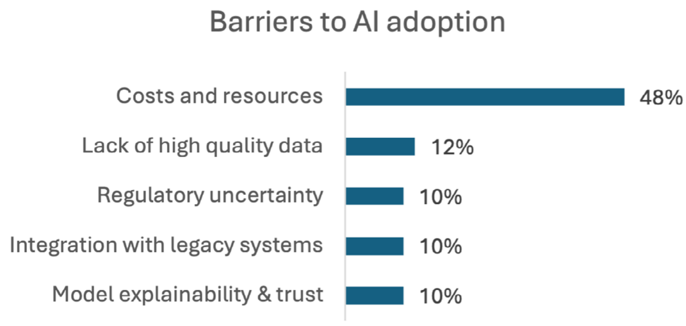
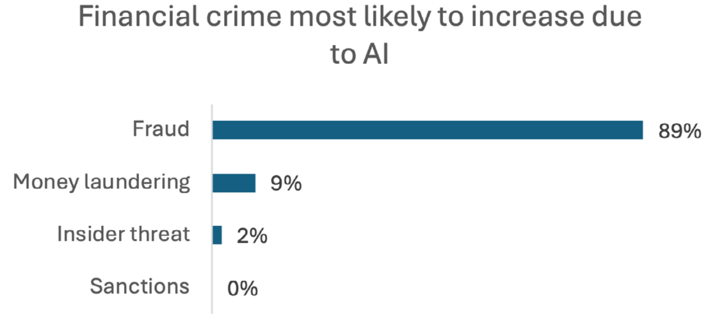


Figure 2: Participant questionnaire, October 1, 2025



AI and financial crime – industry and regulatory perspectives on risk

Workshop participants identified five AI-related threats that could worsen financial crime: constrained resources, cybersecurity issues, low barriers to entry for threat actors, challenges in Canada's regulatory framework, and technology and data issues. Each magnifies the risk. Fraudsters are often seen as "10 steps ahead," while financial institutions remain largely reactive and focused on firefighting.

Constrained resources

Nature of the risk

Participants identified that constrained investment in AI adoption and implementation, and addressing skills gaps, will hinder efforts to combat financial crime.

1. *Competing AI objectives*

Forum members expressed concern that cost-cutting would surface as a preferred short-term objective. They strongly emphasized that deterrence is best improved by prioritizing AI investments focused on enhanced effectiveness before concentrating on AI investments that would produce efficiency gains.

2. Failure to pursue measurable results

Participants discussed that firms adopting AI just because it is the latest trend are likely to fail in both technological development and in their efforts to deter financial crime. Participants stressed their firm belief that AI should be adopted based on clear business cases. AI initiatives should deliver measurable ROI. Workshop participants identified the challenge: "The wrong question is 'How do I adopt AI?' The right question is 'How do we use AI to help our business?'"

3. Investment challenges and legacy constraints

Even when focusing on ROI, financial institutions may be constrained from adopting new AI solutions because those solutions are dependent on modernizing legacy systems. For some, especially smaller institutions, the resources needed for modernization can be challenging, particularly when compared to other investment priorities.

4. AI skill and literacy shortages

Limited access to AI expertise or literacy creates vulnerabilities, which can hinder the deployment of appropriate AI technologies and restrict the institution's capacity to evaluate the benefits of AI adoption. Additionally, the impact of AI on entry-level employees could challenge the skills-development pipeline necessary for building expertise in financial crimes, which has historically benefited from an apprenticeship model.

5. Firm size affects risk exposure

Smaller financial institutions with limited capacity to invest in AI technology are more vulnerable to AI-driven cyber or insider threats, which shift institutional and consumer risk toward these smaller players. The disparity with larger institutions may lead to exploitation by threat actors, who use smaller institutions as entry points, thereby increasing institutional or potentially systemic risk.

6. Constraints on governments and regulators

Canadian governments and regulators also face resource challenges and this could slow AI adoption in government, both with reference to the industry and threat actors. Slow AI adoption could limit Canada's federal and provincial financial regulators, law enforcement, and the judicial system in their efforts to identify, prosecute, and convict criminals.

Cybersecurity issues

Nature of the risk

The rapid growth of AI-enabled cybersecurity risks, such as deepfakes, sophisticated phishing and synthetic identities (a fraud risk where criminals combine real and fabricated data), is increasing the impact and threat of financial crime against both individuals and financial institutions.

1. Increasing personalization

AI-enhanced cyber incidents, often leveraged by social media manipulation, have enabled threat actors to deliver increasingly "personalized" fraud attacks on individuals, making these events increasingly malicious and harder to detect or avoid.

2. Increased cross-border events

AI advancements compound the already significant cross-border challenges in financial crime. Threat actors using AI from abroad face lower detection and prosecution rates, and information sharing across borders is more limited.

3. Insider threat actors and data access

AI-enhanced cybersecurity threats create new opportunities for insiders to become threat actors. Insiders may exploit control and governance gaps to access private consumer or proprietary commercial data. AI-enhanced cyber capabilities among threat actors also raise the risk of organizations hiring individuals whose goal may be to compromise the data integrity of financial institutions or government regulators.

4. Erosion of trust

Participants noted that AI tools are making it increasingly difficult to distinguish genuine communications and identities from fabricated ones, eroding public trust in financial and other institutions.

Low barriers to entry for threat actors

Nature of the risk

Subject matter experts on financial crime at the workshop stated that AI has led to the “democratization of technology,” as individuals no longer need to rely on advanced technology skills or large organized criminal networks.

1. Ease and frequency of use

AI’s accessibility has lowered barriers for threat actors, resulting in those with limited skills now being able to effectively use AI. Low barriers allow for increased frequency of attacks, improve the ability to conceal information, and significantly broaden their reach. AI has also facilitated the emergence of fraud-as-a-service (FaaS), following the same pattern as “software-as-a-service (SaaS),” boosting effectiveness and frequency. Moreover, AI has eliminated the need for foreign language knowledge, which previously posed a significant obstacle to cross-border financial crime.

2. Asymmetrical financial costs

Workshop participants emphasized the imbalance between the relatively low financial cost and risk of carrying out AI-driven attacks, sanctions evasion, or money laundering, and the higher expense and effort required by financial institutions to counter this threat.

Challenges in Canada’s regulatory framework

Nature of the risk

Workshop participants identified challenges in Canada’s regulatory regime that could create barriers to AI adoption, potentially hindering the identification, reporting, and conviction of perpetrators of financial crime. Canada’s federal structure and constitutional division of powers mean that no single jurisdiction, elected or public official, ministry, or agency possesses authority from detection and reporting through to prosecution and conviction. This complexity makes coordination and information sharing more challenging.

Regulatory maturity and compliance risks

Participants observed that the pace of AI adoption by threat actors is accelerating. In parallel, Canada’s financial crime regulatory regime has also evolved. These participants expressed concern about the financial industry’s ability to keep pace with both the increase in AI-enhanced threats and the regulatory changes.

Some forum members emphasized the need for regulatory sandboxes where institutions can test AI without fear of penalties.

Threat actors are increasingly capable of using AI tools to mask the beneficial ownership of corporations, making the need for a comprehensive ownership registry even more critical. While Corporations Canada launched a federal beneficial ownership registry in January 2024, some gaps continue to exist, particularly at the provincial level.

Legal and regulatory frameworks also impact the timely exchange of information among the financial sector, regulators, and law enforcement.

Technology and data issues

Nature of the risk

Three significant technology and data risks were identified related to legacy systems, data integrity, and governance and control frameworks.

1. *Legacy platforms and AI integration - timing and technology challenges*

Nearly all financial institutions face aging legacy systems that sometimes hinder AI integration and lengthen adoption timelines. Forum members described "legacy technology" risk, where criminals exploit these longer adoption timelines as a vulnerability.

2. *Uneven data quality*

Data quality is critical for AI adoption and impacts the quality of AI-enabled analytics. Data quality varies across Canada's financial sector, with fragmented platforms, and is sometimes inconsistent and incomplete. Different classifications and storage methods across banks hinder data sharing. AI models must be trained and operated in this complex environment, which one participant described as the challenge of "building a car while you are driving."

3. *Governance and control frameworks*

Many participants identified that strong and effective governance and control frameworks were the first line of defence against financial crime. The development of AI highlights potential gaps in existing frameworks, such as data access rules that may inadvertently enable data breaches by insider threat actors, the potential introduction of corrupt data, and potential confusion over data ownership when AI creates new linkages. In addition, some financial institutions may place less emphasis on traditional controls when assessing the effectiveness of new AI solutions.

Best practices in financial crime risk mitigation

Forum members identified governance, technology, and operational best practices to mitigate financial crime risk. Best practice should first focus on the fundamentals - risk management, governance and controls.

1. *Maintain effective governance and control frameworks, including but not limited to AI*

Participants described a consistent focus on existing governance and control frameworks as the most effective tool to mitigate AI-enhanced risk. Continued updating will address new AI threats; maintaining emphasis on traditional control mechanisms remains best practice to mitigate AI-enabled financial crimes. For AI governance and control frameworks to be effective, they must be transparent, requiring clear documentation of AI processes to meet board requirements, management objectives, and regulatory risk standards.

2. *Ensuring data quality and data access*

A key principle in combatting financial crime is to ensure that data is accurate, accessible, and "fit for purpose". Data quality will only meet this standard with continued investments in resilient data infrastructure. One potential investment is in accessible, comprehensive, and expanded federal and provincial corporate registration databases that will assist in identifying beneficial ownership connections and combatting AI-related financial crime.

3. *Continued investment and adoption of effective AI tools*

Continued investment in AI tools is essential. Effective AI can analyze behaviour patterns, detect complex financial crimes like money laundering and sanctions violations, and perform network analyses for fraud detection. These tools improve authentication and defend against emerging risks like bots in financial crime and monitoring crypto transactions, as such platforms are used to transfer funds. As participants noted, continued investments must provide measurable AI benefits and should focus, as much as possible, on effectiveness rather than solely on cost-saving efficiencies.

4. *Ongoing AI education, communication, and training*

AI education and training are vital investments for the financial sector, policymakers, and regulators. Upskilling should be a top priority to maintain infrastructure security against threat actors. Training and empowering staff should also be a priority to foster the deployment of AI tools that enhance effectiveness and efficiency. Financial institutions can also offer AI literacy skills to their stakeholders, including customers, to increase awareness of both opportunities and risks. Equally important, best practices recommend that the board and executive management have AI literacy, so that decision-makers can understand AI capabilities, risks, and limitations.

5. *Scaling AI deployment*

Financial institutions can enhance operational resilience by scaling AI deployment. Best practice recommends that scaling starts with identifying pilot or foundational opportunities, moves to broader operational initiatives, and finally concentrates on strategic investments—a so-called “crawl, walk, run” approach.

Opportunities to detect and restrict financial crime

Forum participants identified forward-looking opportunities to minimize financial crime and mitigate the risks associated with AI adoption.

1. *Augmented AI adoption and implementation*

- Technology infrastructure modernization that would include updating legacy systems, modernizing data infrastructure, standardizing data formats, and consolidating data across vendors for unified access.
- Real-time risk assessment allowing deployment of AI at touchpoints and onboarding to support staff decisions and boost defences.
- Automating Suspicious Transaction Reports (STR) and deploying AI for pattern recognition would improve quality and consistency while reducing analyst burden.

2. *Organizational transformation*

- Participants suggested that the financial sector could benefit from directing its investments to increasingly strategic and analytical improvements. Contributing factors include continued investment in AI talent, creation of cross-functional financial crime teams, and focus on strategic transformation rather than “AI quick wins.”
- For governments, significantly increased collaboration would increase effectiveness and efficiency and facilitate cross-pillar coordination.
- Cross-pillar collaboration emerged as a top priority, and some participants suggested that greater central coordination, potentially through a dedicated lead or coordinating

body, could strengthen Canada's approach to financial crime.

- Just two weeks after this workshop, the Prime Minister announced that the November 2025 budget will introduce a "National Anti-Fraud Strategy" complemented by a Financial Crimes Agency to "lead Canada's efforts in combatting sophisticated financial crimes."[i] These announcements will potentially address some of the gaps in coordination and information exchange identified by workshop participants.

3. *Regulatory initiatives*

- Sandboxes and testing environments should be implemented urgently. To address the risks of AI solutions failing to meet regulatory requirements, workshop participants strongly urged regulators to develop and provide a qualified sandbox model. This model should offer a safe harbour for testing innovative AI tools and methods, such as running them in parallel with existing systems during implementation.
- As AI elevates the ability to mask corporate relationships, participants recommended that the current 25% ownership test be reduced, and the definition be broadened to include "control and influence." This could include access to data that makes officers, boards and investors more transparent.
- While privacy was out of scope for this workshop, a number of participants noted that privacy has a significant impact in the fight against AI-assisted financial crime, notably in information sharing. Changes to the privacy regime may be required to balance individual privacy rights with the speed of collaboration needed to combat AI-enhanced financial crime.

4. *Establish a Three-Pillar Collaborative Regime*

- Sixty percent of participants in this workshop responded that joint intelligence efforts between industry and government would best improve public/private collaboration on AI and financial crime.[ii]
- Forum members acknowledged the importance of greater cooperation among financial institutions, regulators, and law enforcement. This should facilitate timely sharing and receipt of accurate and actionable data to counter the use of AI by threat actors to mask funds and hide links, increasing fraud frequency and severity.

NEXT STEPS

Participants in this second FIFAI II workshop brought their insight and subject matter expertise to support a collaborative effort to better understand how AI adoption in the financial sector and by threat actors will affect risk. They further concluded that collaborative initiatives like FIFAI II are an important contributor to advancing the joint interests of the financial industry and its regulators. Their deliberations also identified current best practices to reduce known risks as well as opportunities for both industry and government that would significantly advance Canada's capacity to detect and deter financial crime.

Given the rapid pace of development of AI and AI-assisted financial crime, continued investment and discussions in this area are required by industry, regulators and government simply to keep pace with the bad actors in this area. Significant improvements in AI implementation, industry and regulatory

i News Release, October 20, 2025, Department of Finance Canada. "Minister Champagne takes aim at financial scams and abuse, announces Anti-Fraud Strategy and new Financial Crimes Agency."

ii Participant survey results, Financial Forum on Artificial Intelligence II – Financial Crime, October 1, 2025.

action, and improved collaboration would help protect Canadian consumers and the Canadian financial system.

Two more round tables in this phase of the Financial Institution Forum on Artificial Intelligence will be held in October and November 2025. Interim reports for each of those workshops will be released, followed in 2026 by a final report that will synthesize the forum's perspectives on risks, threats and opportunities.

FINTRAC and GRI appreciated the input of all forum participants and will keep fostering collaborative discussions among industry, policymakers, regulators, and supervisors.

Financial Industry Forum on Artificial Intelligence II:
A Collaborative Approach to AI Threats, Opportunities, and Best Practices Workshop 2 - Financial Crimes
IN4-35/2-2026E-PDF
ISBN 978-0-660-79418-1