Fintechs Canada

Department of Finance
90 Elgin Street
Ottawa ON K1G 0G5

April 28, 2026

On behalf of Fintechs Canada, thank you for the opportunity to comment on the government's consultation on Canada's National Anti-Fraud Strategy.

Fintechs Canada is the unified voice for the most innovative financial technology companies. Serving millions of Canadians daily, our more than 50 members include market-leading Canadian fintechs, fintech-friendly financial institutions, technology companies that power the credit union space, and global fintech companies. Our mission is to make Canada's financial sector more competitive and innovative while strengthening its stability and security.

Fraud in Canada is becoming more complex and increasingly difficult to detect. In the payments sector alone, almost 13% of Canadians have experienced payment-related fraud over a six-month period in 2025, while reported fraud incidents in Canada have nearly doubled over the past decade. With the growing digitization of payments and the increased sophistication of artificial intelligence, fraud will likely continue to grow in complexity.

Fintechs are building the very tools that can strengthen Canada's resilience against emerging threats, through real-time monitoring, AI-driven detection, and enhanced identity verification. Our industry's digital-first expertise is vital to supporting a technology-driven framework that is effective, adaptable, proportionate, and workable in practice. Moreover, fintechs operate on flexible, modern technology stacks that enable rapid deployment of real-time analytics and automated safeguards, enhancing the system's ability to detect and respond to threats as they emerge.But this alone will not be sufficient in a world where scams and fraud routinely cut across sectors, channels, and borders.

We agree with Canada's direction of travel in recognizing that tackling these risks

requires a broader, ecosystem-wide response, not just point solutions. A genuinely effective framework must therefore embed multi-sector coordination that mirrors the sophisticated reality of modern fraud by bringing together financial institutions, telecommunications providers, digital platforms, technology firms, and law-enforcement agencies around shared standards, shared intelligence, and shared accountability to specifically focus on the new scam vectors that bypass conventional security.

Only by aligning incentives, clarifying roles, and enabling secure data-sharing across this wider ecosystem can Canada close the gaps that scammers exploit and ensure that stronger controls in one sector are not simply bypassed via weaker links elsewhere. As the government develops this framework, it is essential that Fintechs are integrated into these foundational conversations.

Below are our responses to selected consultation questions. We welcome the opportunity to continue engaging with the government as the framework is developed, sharing perspectives from Canada's fintech sector.

Oversight

What role could a central regulator play in a Multi-Sector Anti-Fraud Framework? What role could sector-specific regulators play? How can effective oversight be achieved without duplication of existing oversight ?

A central authority should coordinate the framework by setting overall direction and enabling collaboration across sectors. Sector-specific regulators should remain responsible for oversight and implementation within their verticals, leveraging their expertise in sector-specific risks, operational realities, and existing frameworks. These should support the central regulator with enforcement, while ensuring there is no duplication of responsibility or supervisory activities.

To avoid duplication, the framework should build on existing regulatory structures and clearly define each authority's role. Regulatory mandates might require review to align with the new framework. New requirements should complement, not replicate, existing obligations. Organizations should not face overlapping reporting requirements or repeated requests from multiple authorities for the same fraud data, incident information, or compliance documentation.

Compliance requirements should be risk-based and avoid creating a disproportionate burden, particularly for smaller and emerging firms. For firms already regulated by FINTRAC (under the PCMLTFA) or the Bank of Canada (under the RPAA), the Framework should prioritize regulatory convergence. To prevent duplicative reporting, a "single-window" approach is recommended so that Money Services Businesses (MSBs) and Payment Service Providers (PSPs) are not navigating conflicting mandates from multiple authorities for the same compliance activity.

Information Sharing

When should fraud-related information be permitted to be shared, and what information should be shared? What safeguards should be in place?

Effective fraud prevention depends on timely and actionable information sharing within and across sectors. Because modern fraud often spans financial services, telecommunications, and digital platforms, organizations need clear rules on the scope and purpose of information sharing. Any framework should establish clear definitions, requirements, and safeguards, developed in consultation with affected sectors to ensure the rules are technologically practical and responsive to evolving risks.

Current legislative frameworks fail to adequately support this objective. Laws such as the Personal Information Protection and Electronic Documents Act (PIPEDA) and the Bank Act create uncertainty around the sharing of fraud-related information in ways that do not reflect how modern fraud operates. For example, PIPEDA's lack of a clear fraud definition can restrict the sharing of critical victim-related information. As fraud schemes become more sophisticated and involve multiple actors across sectors, these constraints make it harder to identify patterns, detect coordinated activity, and respond quickly.

This fragmented oversight across multiple regulatory agencies creates significant reporting gaps and stifles cross-sectoral collaboration. For example, when a fintech identifies suspected fraud, intermediary financial institutions lack a clear pathway to act due to privacy concerns that restrict their information sharing to other traditional FIs. Despite being on the front lines of financial crime, fintechs remain largely excluded from the critical data-sharing networks essential to industry-wide security and consumer protection.

The framework should build on the domestic private-to-private information sharing mechanism already established under section 7(3)(d.2) of PIPEDA and section 11.01 of the PCMLTFA, rather than creating a parallel structure. However, the current regime is not designed for scale, with each sharing arrangement requiring its own OPC-approved Code of Practice, which creates significant overhead and limits how quickly the network can grow. A single sector-wide Code covering fraud indicators would be a more practical foundation for the cross-sector coordination the Strategy is aiming for.

Legislative amendments are needed to authorize or even oblige organizations to share relevant sector-specific data, risk indicators, and, where appropriate, personally identifiable information, subject to clear privacy safeguards. Organizations and their employees should also be protected by robust safe harbour provisions when sharing information in good faith and in accordance with the framework.

What privacy safeguards or oversight mechanisms should be in place for such information sharing initiatives?

Modernizing privacy frameworks to enable effective fraud prevention requires establishing clear, statutory exemptions for the collection and use of biometric, device, and personal data when used strictly for anti-fraud purposes.

Canadian privacy frameworks must distinguish between static (higher-risk) biometrics and lower-risk dynamic behavioural data, such as keystroke patterns or typing speed. Furthermore, the framework should eliminate the requirement for optional, opt-in consent for the collection and use of data that is critically necessary for real-time fraud detection. Requiring optional consent is counterproductive, as it allows malicious actors to opt out and circumvent essential defenses. We recommend a statutory exemption permitting data use under a "security necessity" basis that overrides general optional consent when data is used strictly to protect customers and the integrity of the financial system.

To be truly effective, provincial and federal privacy legislation must be harmonized. As financial institutions operate nationally, harmonized rules are essential to avoid a multi-jurisdictional compliance burden that impedes or significantly slows down the deployment of nationwide anti-fraud measures.

A predictable industry standard should apply to all participants, ensuring that high privacy standards are maintained without sacrificing the agility needed to combat evolving threats.

When should regulated private sector organizations be able to share fraud-related information with each other? If so, what precise information should be shared, under what circumstances should it be shared and for what precise purposes should it be shared?

Regulated private sector organizations should be empowered to share information when fraud or scam incidents reach a threshold of materiality, ensuring that significant threats are met with a coordinated industry response. Beyond individual cases, sharing should be permitted when specific fraud trends are identified, allowing for proactive defense. By prioritizing the sharing of trend-based data alongside material incident reports, the private sector can move from a reactive posture to a preventative one, closing the visibility gaps that modern scammers currently exploit across the ecosystem.

Prevention

How should organizations be required to embed compliance with the Framework into their governance models?

Fraudsters are adapting quickly, using current events and new technologies to make scams more credible and harder to identify. Seventy-nine percent of Canadians believe artificial intelligence is helping create more convincing scams, 58 percent report experiencing tariff-related scams, and 24 percent have encountered scams tied to cost-of-living pressures. These trends show how quickly fraud is evolving and why static requirements may be ineffective.

Traditional prevention measures are not always sufficient in this environment. Manual or visual checks can be vulnerable to increasingly sophisticated tactics, including AI-generated identities and high-quality document forgeries. Prevention requirements should therefore be principles-based, flexible, and proportionate to the size, risk profile, and services offered by each organization. Organizations should be expected to embed fraud prevention into their governance and risk

management frameworks, but the framework should allow them to adapt their controls to changing risks and operational realities.

Essential to Canada's anti-fraud strategy will be an approach that prioritizes mitigation before a fraudulent transaction occurs. Broader industry and cross-sector coordination is essential to achieving this goal.

Detection

4. How should organizations be incentivized or required to detect and investigate fraud?

Effective fraud detection depends on timely monitoring and intervention. Organizations should be able to use tools such as artificial intelligence and advanced analytics to identify emerging fraud patterns and respond quickly. As fraudsters increasingly use these technologies themselves, regulatory frameworks should not limit their use by legitimate actors.

A primary pillar of this detection strategy should include pre-payment verification, which serves as the critical first line of defense in a modern security stack, ensuring that funds are directed to legitimate recipients rather than diverted to fraudulent accounts through social engineering or identity theft.

While payee verification exists in a rudimentary form, it currently functions as a reactive measure rather than a preventative one. In the case of domestic payments, the fintech industry can often trace and return payments when names and accounts don't match, but this typically occurs only after the fact. By transitioning to a real-time payee verification system, fraudulent transactions could be intercepted and blocked before they are processed, effectively neutralizing a significant portion of payment fraud at the source.

This is even more critical in the case of cross-border transfers, which are operationally final once funds leave the jurisdiction, making recovery an unrealistic option. The framework should therefore prioritize pre-payment prevention measures, particularly in the remittance sector, where post-transaction response measures offer limited recourse.

Prevention must also start further upstream, well before a payment is ever initiated, by tackling the digital environments where scams originate, spread, and ultimately

lead to authorized push payments. A modern framework should incentivize and enable proactive scam detection, supported by timely information-sharing with PSPs and law enforcement. By disrupting scam journeys at their source, upstream measures can significantly reduce the volume of risky payment instructions to ever reach the financial system.

To support these efforts, Know Your Customer (KYC) methodologies should apply across all sectors that provide or facilitate access to financial services. By combining enhanced KYC with robust transaction monitoring, the framework can empower organizations to act swiftly to stop threats.

Liability

5. What responsibilities should organizations have in responding to fraud, and how should liability be structured?

Liability frameworks should reflect how scams occur in practice. Unlike unauthorized fraud, scams do not usually involve an account being accessed without the customer's knowledge. Instead, they involve a customer being deceived into authorizing a payment in good faith. As a result, the payment may appear legitimate to legacy systems even when it was induced by sophisticated fraud.

This distinction is critical because scams often begin far upstream from the payment itself, originating on digital platforms, telecommunications networks, or messaging services. By the time the payment is made, the harm may already be well underway. In these cases, responsibility does not rest only with the payment provider, because multiple actors may have played a role in allowing the scam to reach the consumer.

Liability frameworks should therefore reflect shared responsibility across the entire ecosystem. Assigning liability exclusively to one sector risks weakening incentives for other actors to prevent and disrupt fraud at the source. Ultimately, fraud prevention and detection must be viewed as a shared responsibility across ecosystem participants.

Regulatory clarity, especially around concepts such as "authorized use," "necessary precautions," or consumer fault, will be essential to a predictable framework. Abrupt liability shifts can lead to unintended consequences, including

higher false positives, transaction friction, and potentially increased fraud attempts if reimbursement is perceived as automatic, which undermines the collective goal of strengthening Canada's financial resilience.

Awareness

How can the government improve Canadians' awareness of the threat posed by fraud and better position them to protect themselves against fraud?

Improving national resilience requires a balanced approach to awareness that empowers and protects consumers without shifting 100% of the responsibility to industry participants. Consumers must retain a degree of responsibility, particularly in the context of authorized push payment (APP) fraud. While the framework must prioritize robust technical protections, the government should implement measures that maintain a model of shared accountability.

Canadians should be able to access real-time tools and resources that allow them to understand the mechanics of modern scam archetypes and what they can do to protect themselves.

***

Thank you again for the opportunity to comment. We appreciate the government's leadership in advancing a coordinated approach to fraud prevention and look forward to continued engagement as the strategy is developed. Fintechs are actively contributing to fraud prevention across the ecosystem and stand ready to support the government in developing an effective and responsive framework.

Sincerely,

Adriana Vega
Executive Director, Fintechs Canada