carahsoft.
TECHNOLOGY BY POLICY

The Canada National Anti-Fraud Strategy

A Roadmap for Prevention and Enforcement

October 20, 2025

Overview

Canada's National Anti-Fraud Strategy was announced on October 20, 2025, as part of Budget, in response to a sharp escalation in scam activity **$643M** in reported fraud losses in 2024, with significant underreporting. It sets the stage for a more coordinated federal approach to fraud prevention heading into 2026, emphasizing cross-sector collaboration among financial institutions, telecom providers, and technology firms, alongside stronger consumer controls. Backed by planned Bank Act amendments, the strategy would require banks to strengthen fraud-risk policies, obtain express customer consent before enabling high-risk account features, and give customers tools like transaction limits, while improving fraud data reporting to federal oversight bodies. In parallel, the government plans to establish a new Financial Crimes Agency, with legislation targeted by Spring 2026, to investigate sophisticated financial crime and support recovery of illicit proceeds signaling a shift toward treating fraud as a national enforcement and resilience priority.

Pillar Priority	Directives
Pillar I: Strengthen Bank Fraud Controls	The federal government is advancing measures to make fraud prevention more consistent across financial institutions—requiring stronger bank-led fraud risk management and clearer customer controls for high-risk account features and transfers. **Impact:** Increased demand for fraud analytics, identity/verification, transaction monitoring, and customer-control tooling that reduces scam losses and improves user safety.
Pillar II: Improve Fraud Intelligence and Coordination	Canada is prioritizing better fraud data collection and reporting (including to regulators), paired with broader coordination to disrupt scams across sectors (banking, technology, telecommunications). **Impact:** More need for data-sharing workflows, reporting dashboards, secure collaboration, and case-management systems that connect signals across organizations.
Pillar III: Expand Financial Crime Enforcement Capacity	The strategy signals a stronger enforcement posture by standing up new capabilities to investigate sophisticated financial crime and support recovery of illicit proceeds, alongside clearer expectations for institutional response practices. **Impact:** Opportunity for vendors supporting investigative case management, digital forensics/eDiscovery, secure data environments, and financial crime analytics

Timeline: Key Dates and Milestones

October 20,2025

Government announces Budget 2025 measures launching Canada's National Anti-Fraud Strategy, including proposed Bank Act updates to strengthen bank fraud controls, add customer consent/limits for high-risk features.

November 4, 2025

Budget 2025 is tabled, formally setting the policy agenda and detailing the government's plan to develop and implement the National Anti-Fraud Strategy.

Spring 2026

Government plans to introduce legislation to stand up a new Financial Crimes Agency to investigate sophisticated financial crime and support recovery of illicit proceeds.

Defining Success

As Canada's National Anti-Fraud Strategy moves from announcement to implementation, success will be measured by whether the federal government and regulated sectors can **reduce scam losses, disrupt fraud networks faster**, and **improve consumer protection outcomes** without slowing legitimate payments and digital services. Practical indicators include more consistent fraud controls across institutions, clearer customer protections for high-risk transactions, and stronger visibility into fraud trends through improved reporting and shared intelligence.

Over time, durable success will depend on building the operational capacity to act quickly better coordination across banks, telecom providers, platforms, and law enforcement; faster "freeze and trace" workflows; and stronger investigative capability to pursue complex, cross-border schemes and recover proceeds.

Actions Underway

The strategy is being operationalized through early measures focused on bank controls, reporting, and enforcement enablement. This includes strengthening institutional fraud prevention practices, expanding customer controls for high-risk features and transfers, and improving the quality and consistency of fraud data provided to oversight bodies.

In parallel, the federal government is advancing a more coordinated approach to disruption, supporting cross-sector collaboration and moving toward enhanced investigative capacity to tackle sophisticated fraud at scale.

State and Local

- **Law enforcement collaboration:** Expect more pressure to improve local-to-federal pathways for referrals, evidence handling, and faster coordination with banks and telecoms on active fraud cases.
- **Consumer protection alignment:** Provinces/territories may align guidance and victim-support processes to reduce fragmentation and improve outcomes for consumers.
- **Operational interoperability:** Greater need for shared case workflows, secure information exchange, and common definitions for fraud typologies and reporting.

Bottom Line: Local execution will matter fraud disruption improves when frontline reporting, response, and coordination are consistent across jurisdictions.

Growth Potential

- **Fraud prevention platforms:** Transaction monitoring, behavioral analytics, mule-account detection, and real-time risk scoring.
- **Identity and account security**: Stronger onboarding, authentication, and step-up verification for high-risk actions and transfers.
- **Case management + data sharing:** Investigation workflows, secure collaboration, and reporting dashboards for institutions and regulators.
- **Telecommunication and digital protections:** Scam call/text filtering, spoofing mitigation, takedown support, and threat-intel integration.
- **Managed services:** Fraud operations support, incident response playbooks, and compliance reporting assistance.