Prosper Canada

SUBMISSION

National Anti-Fraud Strategy

April 28, 2026

Contact
Lisa Rae
Director, Systems Change
Prosper Canada
lisarae@prospercanada.org
www.prospercanada.org

Prosper Canada – Who we are

Prosper Canada is a national charity driving bold change that enables more people to prosper. With government, business and community partners across Canada, we expand life-changing financial empowerment services, innovate for greater inclusion and impact, and remove barriers to financial well-being for people with low and modest incomes. Our goal is a Canada where everyone has the opportunity and support they need to achieve financial well-being and live with dignity, stability, and possibility.

Supported by a $60 million investment from the Government of Canada's *Social Development Partnerships Program* – Children and Families (ESDC), in 2025 Prosper Canada launched *Resilient Futures*, which funds 97 community organizations across Canada to deliver proven, free, high-quality financial empowerment services, including tax filing, benefit assistance, and financial education, coaching and counselling. The program is expected to reach 1 million Canadians over four years, connecting them to an additional $2 billion in unclaimed tax and benefit income.

This submission is a component of Prosper Canada's *Advancing Financial Well-being and Protection for Low-Income Canadians* project and is funded in part by Innovation Science and Economic Development (ISED) Canada's *Consumer Protection Initiative*. The views expressed are our own.

Background

In Budget 2025, the government committed to protect Canadians from fraud by developing Canada's first-ever whole-of-government National Anti-Fraud Strategy.

This consultation seeks feedback on proposed measures for a National Anti-Fraud Strategy designed to enhance anti-fraud efforts across Canada's financial and telecommunications sectors, as well as digital platforms. This work is being led by the Department of Finance Canada, in collaboration with other federal departments and agencies.

The consultation seeks views and feedback on:

- Establishing a multi-sector, anti-fraud framework with new and enhanced requirements for federally regulated financial institutions, telecommunications service providers, and digital platforms to prevent, detect and disrupt fraud and to respond to fraud losses when they occur;
- Empowering Canadians to act against fraud; and,
- Supporting law enforcement efforts to combat fraud.

Introduction

Prosper Canada welcomes the Government of Canada's commitment to developing a whole-of-government, multi-sector *National Anti-Fraud Strategy*. Fraud has become a pervasive and rapidly evolving threat to Canadians' financial security, trust in essential systems, and overall financial well-being.

In 2025, 27,693 Canadians lost a reported $704M to fraud with reported losses since 2022 now surpassing $2.4 billion. The Canadian Anti-Fraud Centre estimates that this represents just 5-10% of fraud cases because most go unreported.

The views expressed in this submission are rooted in evidence and insights we have acquired through research and ongoing dialogue with consumer protection stakeholders and our community partners across Canada who work firsthand with low-income and vulnerable financial consumers to help them to build their financial capability, stability, and well-being. This includes empowering them to protect themselves from financial predation, fraud and scams that often target low-income communities, Indigenous communities, newcomers, youth, seniors, and people living with disabilities.

These experiences consistently demonstrate that fraud:

- Disproportionately impacts people with low incomes, seniors, newcomers, people with disabilities, who lack the financial cushion to weather the shocks caused by fraud.
- Frequently uses diverse communication channels (phone, text, email, online ads, online marketplaces, social media, etc.)[1] and exploits security gaps within and between financial sector, telecommunication, social media, and government service systems;
- Causes harms that extend well beyond financial loss, including housing instability, food insecurity, loss of trust in public institutions, and long-term disengagement from mainstream financial services.

Additionally, we reviewed the G20/OECD High-Level Principles on Financial Consumer Protection, and the work of the Aspen Institute's National Task Force on Fraud and Scam Prevention.

[1] A sample list of the types of fraud experienced by people with low incomes, provided by a Prosper Canada community partner:

- **CRA/government impersonation scams:** "You owe taxes, pay now or be arrested."
- **Predatory lending & payday loan fraud:** Finding people denied traditional credit; "Guaranteed approval" loans with hidden fees stripping borrowers of funds.
- **Rental & housing scams:** Fake listings on digital platforms that require upfront damage deposits for properties the scammer doesn't own.
- **Domestic violence and/or economic abuse financial fraud:** opening credit in survivor's or children's name, destroying credit scores
- **Employment & job offer scams:** "Work from home" cheque-washing schemes
- **Digital banking & e-transfer fraud:** Interac e-Transfer intercept scams, fake bank alerts ("your account is compromised, verify now")
- **AI-powered fraud:** AI-generated fake documents
- **Investment fraud:** promises of wealth-building

Based on our analysis, it is clear that fraud is not only a law-enforcement or consumer awareness issue. It is also a **systems failure** that too often leaves individuals—particularly those with low or modest incomes—bearing the consequences of institutional gaps, fragmented oversight, and weak accountability. Our comments emphasize the need to shift risk and the onus for prevention away from individuals and toward the systems and institutions best positioned to prevent, detect, and respond to fraud.

Guiding principles

Prosper Canada's comments and recommendations are guided by the following principles:

1. **Systems should bear responsibility for systemic harm**
   Individuals should not be left to absorb losses or navigate complex redress processes when fraud occurs due to gaps or failures in systems operated by regulated entities.
2. **Prevention, detection, disruption, and response must be inclusive by design**
   Anti-fraud measures must protect consumers without creating new barriers to access, particularly for people with low incomes and vulnerable consumers.
3. **Clear liability and accessible redress are essential**
   Strong prevention measures must be paired with clear accountability, consistent internal complaint handling standards, and the ability to escalate to an external complaints body.
4. **Fraud monitoring, prevention and disruption must be coordinated across sectors**
   Fragmented oversight enables fraud to flourish. Effective responses require coordination, information sharing, and shared responsibility across sectors.

Response to consultation questions

Oversight, scope, and information sharing (*Questions 1–11)*

A National Anti-Fraud Strategy will only be effective if it is designed and governed as a coordinated system-wide response to a problem that routinely spans sectors, jurisdictions, and platforms. Fragmented oversight and inconsistent standards across the financial sector, telecommunications providers, and digital platforms create gaps that fraudsters exploit—often at the expense of individuals least able to absorb the resulting harm.

Scope of the framework (Question 1)

Prosper Canada agrees that federally regulated financial institutions, telecommunication service providers, and major digital platforms are appropriate sectors for the initial phase of a *National Anti-Fraud Framework*. These sectors sit at the centre of how fraud is initiated, facilitated, and monetized, and they exert significant control over the systems and infrastructure that fraudsters rely on.

However, limiting the Framework to a fixed group of sectors risks allowing fraud to migrate rather than be meaningfully reduced. The Framework should therefore be explicitly **expandable**, with a clear mechanism to bring additional sectors into scope where evidence demonstrates material consumer harm. Priority candidates include payment service providers, fintechs, and online marketplaces, that are routinely leveraged in fraud and scam activity.

A flexible and adaptive scope is essential to ensure the Framework remains responsive to evolving fraud mechanisms, tactics and technological change, rather than lagging behind them.

Framework oversight and coordination (Questions 2- 4)

Given the cross-sector nature of modern fraud, Prosper Canada strongly supports the establishment of a **central coordinating authority** with a mandate to take a system-level view of fraud risks and consumer harm. This body should not replace existing regulators or duplicate sector-specific supervision. Instead, its role should focus on:

- Aggregating and analysing fraud intelligence, trends, and consumer outcome data across sectors.
- Identifying emerging, cross-sector, fraud risks and systemic vulnerabilities.
- Monitoring the effectiveness of prevention, detection, and response measures from a consumer harm perspective.
- Coordinating regulatory action where accountability or liability spans multiple regulated entities.

Sector-specific regulators should retain responsibility for enforcement within their mandates, while operating within a formalized coordination structure that reduces duplication, closes gaps, and promotes consistent expectations and outcomes for consumers. Clear governance arrangements, well-defined roles, and routine inter-regulator reporting will be essential to ensure accountability, transparency, and effective oversight.

Effective coordination requires mechanisms that enable banks, regulators, telecommunications providers, digital platforms, and the Canadian Anti-Fraud Centre to learn from one another in near-real time, rather than operating in parallel silos. Information-sharing arrangements should support system-wide learning and prevention, not merely post-incident reporting.

Transparency and accountability would be strengthened by regular, public reporting on fraud attempts, successful fraud, and the effectiveness of prevention and intervention measures across sectors. Consistent, comparable metrics can create feedback loops that support continuous improvement and enable stakeholders to assess whether policy responses are reducing consumer harm over time.
To better understand and address inequitable impacts, fraud-related data should be disaggregated by income and other vulnerability indicators and tracked over time, enabling policymakers to identify which communities are most affected and whether interventions are improving outcomes at the household level.

Information sharing between regulators (Questions 5, 6, and 7)

Effective oversight depends on timely and responsible information sharing. Prosper Canada supports information-sharing authorities that are clearly defined, purpose-limited, and proportional to the risks being addressed. Information sharing between regulators should be permitted where it is demonstrably necessary to prevent, detect, disrupt, or investigate fraud, or to identify emerging systemic risks and cross-sector patterns. Priority should be given to sharing fraud typologies, tactics, trends, and risk indicators, rather than personal data.

Strong safeguards are critical to maintaining public trust and minimizing unintended harm. These should include data minimization requirements, transparent legal authority, auditability, and independent oversight. Special attention should be balanced with reducing the risk of false positives and unnecessary system frictions for individuals whose access to essential services may be affected by anti-fraud interventions.

Information sharing – law enforcement and the private sector (Questions 8–11)

Prosper Canada supports well-defined pathways for regulators to share information with law enforcement where it is necessary to prevent or disrupt active fraud, or to support the investigation of systemic, organized, or cross-border fraud. Such sharing should be grounded in clear legal authority and accompanied by safeguards that protect privacy, procedural fairness, and due process.

Information sharing between law enforcement and private-sector organizations should be more limited and carefully constrained. It should focus on actionable risk intelligence that can materially prevent or reduce harm to individuals, and it should occur only in circumstances where the benefits of sharing clearly outweigh the risks.

Across all forms of information sharing, transparency, accountability, and oversight are essential. Without these safeguards, even well-intentioned anti-fraud measures risk undermining trust in public institutions and essential services—particularly among communities that already face barriers to financial inclusion.

Prevention: governance, training, identity validation, and consumer education (Questions 12–16)

Effective fraud prevention requires more than consumer vigilance or isolated technical controls. As the Aspen Institute's National Task Force on Fraud and Scam Prevention discusses, fraud flourishes when institutional systems are fragmented, incentives are misaligned, and accountability is diffuse. Prevention must therefore be embedded at the **governance, design, and operational levels** of systems that enable financial transactions, communications, and digital engagement.

Governance and organizational accountability (Question 12)

Prosper Canada supports requiring organizations to **embed antifraud obligations into senior governance structures**, including clear executive accountability, board-level oversight, and integration into enterprise risk management. The Aspen Institute's work highlights that sustained reductions in fraud are associated with organizations that treat fraud prevention as a core organizational responsibility, rather than a compliance exercise delegated to siloed teams.

Governance requirements should emphasize responsibility for consumer outcomes, including monitoring whether prevention measures meaningfully reduce harm and avoid disproportionate impacts, including on marginalized or financially vulnerable populations.

Training and institutional capacity (Question 13)

Training requirements must move beyond generic awareness modules. Both Prosper Canada's community partners and the Aspen Institute's Task Force stress the importance of **role-specific, regularly updated training**, particularly for frontline staff who interact directly with consumers experiencing fraud or financial distress.

Training should incorporate:

- Understanding of evolving fraud typologies and tactics;
- Recognition of consumer vulnerability and trauma-informed response; and
- Clear escalation, reporting, referral, and redress pathways.

Effectiveness of training should be evaluated based on outcomes, such as improved detection, reduced consumer harm, and improved experiences for fraud victims.

Identity validation and inclusion (Question 14)

Identity validation plays a critical role in preventing fraud but can also create barriers to access if implemented inflexibly. Prosper Canada supports **risk-based, proportionate identity validation** requirements that are explicitly designed to avoid exclusion of individuals with non-standard documentation, limited digital access, or precarious life circumstances. Particular attention should be given to multi-factor authentication which often assumes that consumers have more than one electronic device (e.g. a smart phone and a computer).

As people with low incomes typically have a smart phone, but not a computer, multi-factor authentication processes should be designed with options for people with only one device (most likely a phone). More generally, consumer protections at the login and transaction level should be tested with diverse consumers -- including those most likely to experience barriers, such as seniors and people with low incomes, language/literacy barriers, and/or disabilities.

The Aspen Institute's analysis underscores that identity tools should focus on trustworthiness and authenticity rather than rigid formal documentation, and that safeguards and rapid appeal mechanisms are essential to address false positives and prevent unjust denial of access to essential services.

Consumer education (Questions 15–16)

Consumer education is necessary but insufficient as a standalone strategy. Education must complement strong system-level protections, not substitute for them.

Consumer education should also include clear, timely, and plain-language communication when transactions or activities are flagged or blocked due to suspected fraud. Proactive notifications—similar to warning systems used in other digital services—can help reduce confusion, reinforce trust, and support learning without stigmatizing individuals or implying fault.

Education requirements should focus on:

- Clear, plain-language information about common fraud risks.
- Practical guidance on how to report suspected fraud and seek redress and why (e.g., it enables more effective fraud detection, disruption and prevention).
- Reducing stigma associated with fraud victimization to encourage reporting.

Effectiveness should be assessed using outcome-based measures—such as increased reporting and reduced harm—rather than reach, impressions, or other passive awareness metrics.

Response: reporting, redress, and liability (Questions 36–45)

When fraud occurs, quality of institutional response can be a decisive factor in determining whether individuals experience recovery or persistent financial and emotional harm. Slow, fragmented, or opaque response processes deepen harm and erode trust, particularly for people with limited financial resilience.

Prosper Canada supports requirements for organizations to provide **simple, publicly accessible, reporting channels**, including digital and non-digital options, with clear guidance on next steps and transparency on response times, as well as information on when and how the consumer may escalate a complaint to a designated external dispute resolution body. Reporting should not require consumers to determine which organization or sector is "responsible" before receiving assistance.

Cross-sector fraud complaints should have a **single point of entry**, with responsibility placed on institutions—not individuals—to coordinate investigations where multiple systems are implicated. Organizations should be subject to clear investigation timelines and required to provide written explanations of outcomes.

Liability for non-compliance (Questions 40–42)

Prosper Canada strongly supports **holding organizations liable** where failure to meet Framework obligations contributes to consumer harm. Fraud thrives when individuals are left to manage the impact of fraud on their own, and the institutions that retain control over the systems that enable fraud, are let off the hook.

Persistently assigning losses to individuals—particularly in cases where consumers are deceived, coerced, or manipulated into authorizing transactions—weakens institutional incentives to invest in effective prevention. Legislative and regulatory frameworks should avoid distinctions that treat "authorized" scam payments as equivalent to informed consumer choice, where authorization is obtained through deception or pressure.

Liability standards should:

- Be clear and enforceable.
- Reflect the proportional contribution of each organization where multiple systems are involved.
- Ensure that individuals are made whole without bearing the burden of navigating inter-institutional disputes.

Clear liability is essential not only for compensation, but also to realign incentives toward prevention and rapid intervention.

Independent external dispute resolution (Questions 43–45)

Prosper Canada supports the creation of a **single independent external complaints body** with authority to hear cross-sector fraud complaints, escalated complaints, issue binding decisions, and help promote consistency in fraud complain handing across organizations and sectors. A single external complaints body is the international standard in consumer protection related to banking and should inform this framework. We strongly uphold that credible redress mechanisms are central to restoring trust and encouraging reporting.

This body should be accessible, independent, and responsible for reporting systemic issues; work in the public interest; and practice transparent public reporting to promote accountability and continuous improvement.

Empowering Canadians to act against fraud (Questions 46–47)

Empowering Canadians to act against fraud requires more than awareness campaigns. Individuals are most likely to act when education is **embedded in trusted touchpoints** and paired with clear, supportive pathways to assistance.

Prosper Canada supports nationally coordinated, evidence-based, education efforts that:

- Are integrated into trusted service environments such as financial institutions, telecom providers, government services, tax filing assistance, benefit delivery, and community financial support services.
- Reduce shame and stigma associated with victimization.
- Emphasize practical actions, including timely reporting and use of redress mechanisms.

Public education should also address the misuse of government-issued identifiers, including Social Insurance Numbers, as a cross-sector risk with both financial and social consequences, particularly for low-income individuals and newcomers.

Supporting law enforcement and strengthening the Canadian Anti-Fraud Centre (Questions 48–50)

Prosper Canada supports measures to strengthen law enforcement capacity and coordination, with a focus on **intelligence, prevention, and disruption of systemic fraud** rather than reliance on individual victim reporting alone. The Aspen Institute's work highlights the importance of centralized intelligence functions and clear feedback loops between institutions, regulators, and law enforcement.

In this context, Prosper Canada supports a reinforced role for the Canadian Anti-Fraud Centre as:

- A national reporting and intelligence hub.
- A coordinator of cross-jurisdictional and cross-sector insights
- A trusted source of public education and trend analysis.

Strengthening enforcement capacity will require **sustained public investment**, particularly for intelligence-led disruption of organized cross-border fraud and fraud facilitated through emerging payment technologies. Consumer-facing education and reporting must be matched by enforcement resources capable of addressing the scale and complexity of modern fraud networks.

Investments in law enforcement should be complemented by safeguards to ensure transparency, proportionality, and protection of consumer rights.

APPENDIX 1
Consultation questions

A Multi-Sector Anti-Fraud Framework

Oversight, Information Sharing and Reporting to Law Enforcement

1. Are the three described sectors appropriate for the initial phase of a Framework? Should other sectors be considered?

2. What role could a central regulator play in a Multi-Sector Anti-Fraud Framework?
3. What role could sector-specific regulators play in the Framework?
4. How can effective oversight of the Framework be achieved, without duplication of existing oversight of the three sectors?
5. When should Framework regulators be permitted to share fraud-related information with each other for the purposes of further the Strategy aims of preventing, detecting, disrupting, and investigating fraud?
6. If so, what specific information should be shared, under what circumstances should it be shared and for what precise purpose should it be shared?
7. What privacy safeguards or oversight mechanisms should be in place for such information-sharing initiatives?
8. When should Framework regulators be permitted to share fraud-related information with law enforcement for the purposes of preventing, detecting, disrupting, and investigating fraud?
9. When should law enforcement be permitted to share fraud-related information with private sector organizations?
10. If so, what specific information should be shared, under what circumstances should it be shared and for what precise purpose should it be shared?
11. What privacy safeguards or oversight mechanisms should be in place for such information-sharing initiatives?

Prevention

12. How should organizations be required to embed compliance with the Framework into their governance models?
13. How can organizations ensure that anti-fraud training is effective and how should this be reflected in government policy or legislation?
14. When, and how, should organizations be required to validate the identity of users of their services?
15. What fraud-related information should organizations be required to make available to individuals using, or who may use, their services?
16. How should the effectiveness of organizations' fraud education be assessed to ensure it meaningfully reduces harm?
17. What sector-specific fraud-prevention rules should be in place?

Detection

18. How could organizations be incentivized to effectively detect and investigate potentially fraudulent activity on their services?
19. How should organizations be required to assess fraud-related harms to individuals using their services?
20. What actions should organizations be required to take to assess risk of future harm to individuals impacted by fraud?

21. When should regulated private sector organizations be able to share fraud-related information with each other?
22. If so, what precise information should be shared, under what circumstances should it be shared and for what precise purposes should it be shared?
23. What privacy safeguards or oversight mechanisms should be in place for such information sharing initiatives?
24. When should organizations be permitted to share fraud-related information with law enforcement for the purposes of preventing, detecting, disrupting, and investigating fraud?
25. When should law enforcement be permitted to share fraud-related information with private sector organizations?
26. When should the government be permitted to share fraud-related information with law enforcement?
27. When should the government be permitted to share fraud-related information with private sector organizations?
28. If so, what specific information should be shared, under what circumstances should it be shared and for what precise purpose should it be shared?
29. What privacy safeguards or oversight mechanisms should be in place for such information-sharing initiatives?
30. What sector-specific fraud-detection rules should be in place?

Disruption

31. How can a balance be struck to limit use of industry infrastructure for fraudulent purposes, while ensuring that legitimate users are not unreasonably cut off from use of services?
32. In what situations should regulated entities be required to pause potentially fraudulent activity?
33. What measures, safeguards and recourse should be put in place to ensure that individuals' access is not improperly suspended or removed?
34. How can notifications of suspected fraudulent activity be effective?
35. What sector-specific fraud-disruption rules should be in place?

Response

36. How should organizations be required to facilitate users' reporting of fraud activity to organizations?
37. How could organizations effectively investigate cross-sector complaints?
38. How long should organizations have to internally investigate complaints?
39. What information should organizations be required to include in a summary of complaint?
40. Should organizations be held liable when they do not fulfill their obligations under the Framework?

41. What standards should apply in determining whether an organization fulfilled its obligations?
42. How should liability be apportioned when multiple organizations have not fulfilled their obligations?
43. What should inform how an external complaint body is chosen?
44. Should decisions of the external complaint body be binding?
45. How long should the external complaints body have to investigate escalated complaints?

Empower Canadians to act against fraud

46. How can the government improve Canadians' awareness of the threat posed by fraud and better position them to protect themselves against fraud?
47. How can the government improve Canadians' awareness about the risk of misuse of government-issued identifiers, including social insurance numbers?

Support law enforcement's ability to combat fraud

48. What can be done to support federal law enforcement's ability to investigate fraud and collect fraud-related intelligence?
49. What should be done to improve coordination between Canadian law enforcement across federal, provincial and territorial and municipal levels, and between those law enforcement bodies and international partners?
50. What role should the CAFC play in advancing the Strategy?

Prosper Canada has received funding from Innovation, Science and Economic Development Canada's Canadian Consumer Protection Initiative. The views expressed in this report are not necessarily those of Innovation, Science and Economic Development Canada or of the Government of Canada.

Funded by the Government of Canada
Financé par le gouvernement du Canada | Canada