

April 28, 2026

Submitted via E-Mail: consumer.consommateur@fin.gc.ca

Judith Hamel
Financial Sector Policy Branch
Department of Finance Canada
James Michael Flaherty Building
90 Elgin Street
Ottawa, ON K1A0G5

Dear Ms. Hamel:

RE: REQUEST FOR COMMENTS - NATIONAL ANTI-FRAUD STRATEGY DISCUSSION PAPER

The Canadian Forum for Financial Markets/ Forum Canadien des Marchés Financiers is a values-driven, purposeful, and reform-minded organization, dedicated to improving the health and competitiveness of Canada's financial markets for the greater good.

We write in response to the Government of Canada's National Anti-Fraud Strategy Discussion Paper (the "**Discussion Paper**") and offer the below comments as a solutions partner to improve the government's proposed anti-fraud strategy (the "**Strategy**"). This response focuses on the financial services sector.

EXECUTIVE SUMMARY

Effective efforts by the Government of Canada to protect Canadians from fraud through useful law, regulation and law enforcement is supported. It necessitates clearly defining the types of fraudulent conduct to be addressed, and drawing upon Canada's existing systems, augmenting only where and how clearly warranted.

The Strategy does not appear to be based on any data or analysis on the occurrence or characteristics of fraud in Canada it seeks to address, which is needed to define its scope and ensure its success. New financial sector requirements and a new regulator risks ineffectiveness, duplication and overlap.

Any liability framework should be fact-specific, grounded in a negligence standard, and based on whether the firm caused the loss. Safe harbour protections should be included for good faith compliance.

Fraud can be undetectable. It is primarily a criminal justice and public-safety issue. Prevention requires involvement from Public Safety and Justice.

Globalized fraud networks highlight systemic issues: under-resourced law enforcement and prosecution, low conviction rates, and the need for integrated international enforcement capabilities.

A data-driven approach is also necessary to identify all relevant victims and sectors, recognizing that fraud proceeds often move through payment processors, e-commerce platforms, retailers, and non-bank financial services.

A streamlined follow-up consultation should be issued centred on strategic issues.

A. DEFINING SCOPE

A series of Consultation Questions (for example Questions 2-4) address the scope of the Strategy and the establishment of a new regulatory oversight framework including an independent regulator (the “**Framework**”).

I) The Need for a Data Driven Approach

The impetus behind the Strategy is to address a noted increase in the scale and sophistication of fraud using new technologies to target Canadians. According to the Discussion Paper, this includes the use of misleading and coercive emails, texts, phone calls, social media posts, and paid advertising to engage with prospective victims and either gain access to a victim’s bank account or deceive/coerce a victim into transferring funds out of their bank account.

Though certain types of fraud may be on the rise in Canada, the Strategy is not supported by any statistics or analysis on, for example, the types of fraud being committed, the Canadians that are most vulnerable to fraud, and/or the origin of fraud in Canada. There is, for example, no statistics or analysis on the prevalence or frequency of any type of fraudulent scheme, the common demographics on Canadian victims, and to what extent the fraudsters that are targeting Canadians are located outside of Canada.

Rather, the Discussion Paper states that, in 2025, Canadians reported losing more than \$704 million to fraud, bringing the total reported losses since 2022 to over \$2.4 billion¹. According to the Discussion Paper, only an estimated 5 to 10 per cent of incidents are reported², making the true impact far higher. Although no citation has been provided, these statistics derive from the Canadian Anti-Fraud Centre (the “**CAFC**”), which collects information on fraud and identity theft

¹ Discussion Paper, page 3.

² Ibid.

in Canada.³ However, the CAFC receives reports and gathers statistics on a wide range of frauds impacting individuals and businesses and, as a result, it is unclear what type of “fraud” has resulted in these reported losses. In addition, it is unclear how the CAFC has estimated that only 5 to 10 per cent of incidents are reported.

In order for the Strategy to have a meaningful impact on Canadians, it must be data focused and include a thorough analysis on the underlying fraud that the Strategy is intended to address. This will help to determine the proper scope for the Strategy, to what extent gaps may exist and the entities best placed to fill them domestically and internationally,⁴ without overlap and duplication.

In the absence of this data and analysis, the purpose of the Strategy and its effectiveness in reducing the occurrence of fraud in Canada is in question.

A fulsome analysis should be completed before adopting a framework or imposing new obligations on regulated firms.

II) The Need for a Refined Scope

As currently drafted, the scope of the Strategy is vague and requires further refinement. According to the Discussion Paper, the initial focus of the Strategy will be on fraud targeting individual Canadians and small organizations and will include any attempt, “regardless of source” and whether or not successful, to:

1. Deceive or coerce an individual into authorizing a payment, transferring funds, or sharing personal or financial information in order to cause loss or harm to an individual;
2. Gain access to or use an individual’s account in order to cause loss or harm to an individual; or
3. Impersonate clients to access federal government accounts or to redirect payments.

This definition not only captures fraudulent schemes that make use of telecommunications, social media, and digital platforms to engage with prospective victims, but could also capture a wide range of ‘traditional’ fraud involving financial institutions including cheque fraud and identity theft. More generally, this definition appears to capture any fraud, misrepresentation, or dishonest act by a third party that results in a victim transferring funds out of their account with a federal bank. This could include, for example, various forms (non) violent conduct in turn resulting in various forms of investment fraud, Ponzi schemes, and ‘romance fraud’ perpetrated by a third party that is known or unknown to the victim regardless of whether the fraud makes use of electronic communications of any kind.

³ [Fraud Prevention Month to bring hidden crime into the spotlight - Canada.ca](#)

⁴ The Discussion Paper states that fraudsters are often not located in Canada, and are able to perpetrate fraud remotely, regardless of international and provincial and territorial borders. (p. 4)

Based on the information included in the Discussion Paper, it is not clear whether the Strategy is intended to cover third-party fraud of any kind that involves a victim's bank account or whether the Strategy is intended to focus on a subset of schemes that make use of social media, telecommunications, or emerging technologies. The scope of the Strategy should be refined to eliminate any ambiguity on its intended outcomes and as noted above, should be driven by data to ensure that it effectively targets the types of schemes that are putting Canadians at risk.

B. THE AVOIDANCE OF DUPLICATION AND OVERLAP

Canada and its federal financial sector have many regulators. The Discussion Paper states that the Framework “could” require regulated organizations to fulfill a set of general obligations reinforced by separate industry-specific obligations and that these requirements “could” supplement, rather than duplicate, existing fraud-related consumer protection measures. If the government proceeds with a strategy in any form, it is imperative to avoid creating duplicative regulatory obligations and/or establishing a new federal regulator.⁵ Canada already has infrastructures to identify, avoid, and mitigate the risks of third-party fraud:

- With respect to the financial services sector, federal banks are already regulated by several entities including the Office of the Superintendent of Financial Institutions, the Financial Consumer Agency of Canada (“**FCAC**”), and the Financial Transactions and Reports Analysis Center of Canada (“**FINTRAC**”). At the provincial level, subsidiary firms are regulated by numerous other regulators including provincial and territorial securities commissions, insurance regulators, and the Canadian Investment Regulatory Organization. These entities create a web of regulatory obligations which include professional conduct standards, reporting obligations, investor protections, and policies and procedures to maintain firm oversight.
- In addition, as noted in the Discussion Paper, the telecommunications industry is already regulated by the Canadian Radio-Television and Telecommunications Commission (“**CRTC**”), which has developed methods to identify and disrupt fraud.
- Across all sectors, with respect to law enforcement, the federal government has announced that it will be establishing a new Financial Crimes Agency to investigate complex cases of money laundering, organized crime, and online financial scams.⁶
- Further, the Royal Canadian Mounted Police, Ontario Provincial Police, and the Competition Bureau of Canada have partnered to support the CAFC to collect information on fraud and identify theft in Canada.⁷

In this context, it is not necessary or prudent to establish a new federal regulator with a mandate

⁵ Consultation Question 50.

⁶ <https://www.canada.ca/en/department-finance/news/2026/02/government-announces-new-measures-to-help-protect-canadians-and-businesses-against-extortion>

⁷ <https://www.canada.ca/en/competition-bureau/news/2026/03/fraud-prevention-month-to-bring-hidden-crime-into-the-spotlight.html>

to address “fraud” or any particular species of fraud.

Rather, Canada’s existing legal and regulatory system should be considered holistically to draw upon existing law enforcement and regulators. For example, should improved coordination and cooperation between industry regulators be necessary, this could be implemented through a memorandum of understanding between regulators.⁸ These measures would accomplish the Strategy’s goals but avoid the substantial risk of regulatory overlap and duplication that would arise from creating a new regulator.

I) The Financial Services Sector

The Discussion Paper identifies prevention, detection, disruption, and response as the primary elements of the Strategy and describes several industry-specific and general requirements that could be included in each of those elements. For example, the Discussion Paper notes that the prevention element of the Strategy could include know-your-client (“KYC”) and investor education requirements, and the detection element of the Strategy could include account monitoring and information sharing. In addition, the disruption element of the Strategy could include freezing accounts and user warnings, and the response element of the Strategy could include streamlined complaint handling processes.

In review of the Discussion Paper, we observe that federally regulated banks are already required or have otherwise adopted many of these measures. For example, banks already have KYC obligations⁹, monitor client accounts, and provide notices to clients to flag suspicious transactions. In addition, banks are already permitted and do in fact provide law enforcement with information on fraudulent schemes involving client accounts. Moreover, federally regulated banks have well-established and regulated complaint handling¹⁰ and external dispute resolution systems.¹¹ As a result, it is not clear that the Strategy is needed to improve the financial sector’s ability to prevent, detect, disrupt, and/or respond to fraud.

The proposed amendments to the *Bank Act* S.C. 1991 c. 46¹² should not be augmented with more prescriptive fraud-specific regulation¹³. Rather, creating prescriptive requirements for each element of the Strategy could have the perverse effect of shifting the primary liability for a fraud from the fraudster to the victim’s bank. Federal banks should have reasonable policies and procedures in place to avoid directly falling victim to fraudsters who, for example, seek to access a client’s account by misappropriating their identity. However, it is important to emphasize that fraud is deceptive by nature and there are practical limitations on a financial institution’s ability to ensure that its clients do not themselves fall victim to third-party fraud. This is especially true in cases involving sophisticated schemes and the use of emerging technologies.

⁸ Consultation Questions 5-11 and 21-29 regarding information sharing include fact and law specific questions for which this consultation is not the effect venue. The Discussion Paper and consultation questions do not acknowledge the information sharing that currently takes place.

⁹ Consultation Question 14.

¹⁰ Consultation Question 37-39

¹¹ Consultation Questions 42-45.

¹² Bill C-15: An Act to Implement Certain Provisions of the Budget Tabled in Parliament on November 4, 2025.

¹³ Consultation Questions 17,35.

C. LIABILITY

Although banks can play an important role in helping their clients avoid fraud, they should not be held liable in all cases where their clients have been deceived or have otherwise provided a fraudster with access to their account or their financial information. Likewise, although banks can adopt systems to identify fraudulent transactions, the evolving nature of fraud and the use of sophisticated schemes and technologies present challenges to identifying and responding to fraud.¹⁴ As such, following proper data review and analysis, to the extent that a strategy includes any further industry-specific requirements for the federal banking sector, that those requirements should be principled based, a bank's liability for those requirements should be fact-specific, based on a negligence standard and a consideration of whether the bank's actions or inactions caused the client's loss. A strategy that includes overly prescriptive rules and/or a system of strict liability would create indeterminant risk for regulated firms and should be avoided. Such an approach raises costs for consumers and renders banks overly cautious in their services and innovations to consumer detriment.

In addition, to the extent that a Strategy requires regulated banks to take proactive measures to avoid fraud by, for example, reporting information to another regulator or law enforcement agency, or to freeze a client account, the strategy must include safe harbour protections for compliant firms. In other words, where a firm take steps to address potential fraud in line with its regulatory obligations, the firm should not be held liable in the event that those measures are alleged to have caused harm to the fraudster or victim. This will ensure that firms are not penalized when complying with their regulatory requirements.¹⁵

D. THE NEED TO REDEFINE 'WHOLE-OF-GOVERNMENT' APPROACH

The Strategy is described as a "whole-of-government" and "multi-sector" strategy to protect Canadians from evolving and highly complex fraud. To that end, the Strategy engages federal regulators and law enforcement agencies and applies to the federally regulated financial and telecommunications sectors. The government's intention of prompting a holistic response to fraud through effective regulation and law enforcement is supported. The following recommendation are provided in support of that goal:

i) **Additional Departmental Focus Needed**

Fraudulent access to Canadian bank accounts is fundamentally a criminal justice and public safety issue, rather than primarily a fiscal or economic policy matter. While Finance excels at bank policies, it does not have investigative powers or police coordination needed to pursue

¹⁴ The Discussion Paper states the advance of sophisticated technology adds complexity to fraudulent acts while facilitating fraudsters' access to tactics and techniques. (p. 4)

¹⁵ Consultation Questions 40, 41

fraudsters, boost convictions and recover funds. Investigation, enforcement and prosecution, as the core to stopping fraud, fall under Public Safety Canada and Justice Canada.

ii) Systemic Issues

Real world fraud chains including overseas syndicates demand integrated global law enforcement that dismantle crime networks. Under-resourced police and prosecution efforts within current systems need to be addressed and conviction rates bolstered.¹⁶

iii) Other Victims

As set out in this correspondence, any approach should be driven by data and reevaluated following an analysis on the types of fraud being perpetrated on Canadians and, by extension, the types of regulated entities that are impacted by those schemes. Though the Discussion Paper refers broadly to undefined digital platforms, the movement of fraud proceeds may also occur more specifically, for example, through payment processors, e-commerce platforms, retailers and other regulated financial industries apart from federally regulated banks.

E. A STREAMLINED CONSULTATION

It is recommended that a streamlined consultation be issued considering the issues raised in this correspondence. The consultation need not include fact specific, operational questions that firms are best placed to address internally¹⁷

Respectfully submitted,

The Canadian Forum for Financial Markets

www.CFFiM-FCMFi.ca

¹⁶ Consultation Questions 48-49.

¹⁷ For example, Consultation Questions 12 (Governance), 15, 16 (Education) 18 (Detection), 19, 20 (Impact), 31, 32, 33, 34, 36 (General Requirements)