OBSI OMBUDSMAN FOR BANKING SERVICES AND INVESTMENTS
OSBI OMBUDSMAN DES SERVICES BANCAIRES ET D'INVESTISSEMENT

May 1, 2026

Delivered by email to: consumer.consommateur@fin.gc.ca

Judith Hamel
Financial Sector Policy Branch
Department of Finance Canada
James Michael Flaherty Building
90 Elgin St
Ottawa ON K1A 0G5

Re: Response to the National Anti-Fraud Strategy Consultation

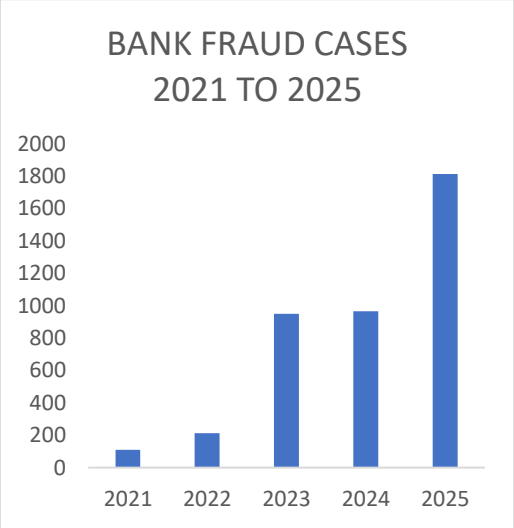
The Ombudsman for Banking Services and Investments (OBSI) is pleased to provide our comments to the Department of Finance Canada in response to its recent consultation, *National Anti-Fraud Strategy Consultation*.

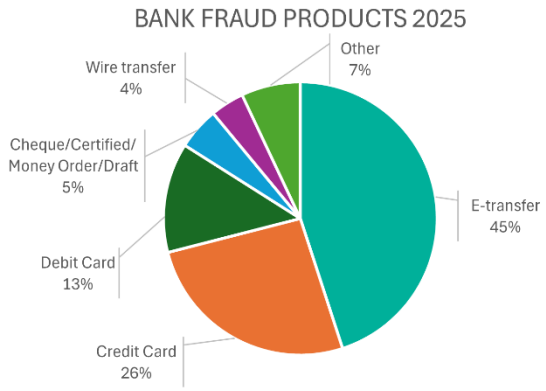
OBSI is a national, independent, and not-for-profit organization that helps resolve and reduce disputes between consumers and over 1,500 financial services firms from across Canada in both official languages. We provide services to federally regulated financial institutions, provincially regulated securities firms and credit unions from across the country. We have been providing these services for over 30 years. As such, we are uniquely positioned to share our views and insights for this important consultation.

OBSI's experience with fraud

Cases involving fraud, particularly e-transfer fraud and other types of digital fraud, have impacted an unprecedented number of Canadian consumers in recent years. This is reflected in a dramatically increased volume of complaints about these issues that consumers have escalated to OBSI.

In 2021, OBSI opened 110 cases related to bank fraud. By 2022, this number had nearly doubled to 213 cases. Since 2022, we have seen continued, significant increases in banking fraud cases. In 2024, we opened 965 fraud cases and in 2025, we saw this number increase to 1,812 fraud related cases. We are on track to open even more banking-related fraud cases in 2026.





Some of this growth in complaint volume is associated with important 2022 changes to the Bank Act consumer protection framework that reduced complaint attrition at federally regulated banks and our assumption of our role as the single External Complaints Body (ECB) for all federally regulated banks in 2025. However, we note that this increase in banking fraud in Canada also reflects a broader global phenomenon. Financial ombudsman services around the world report similarly significant increases in bank fraud related cases.

Consultation Questions

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

OBSI agrees that the three sectors described are appropriate for the initial phase of the framework. In the cases that we investigate, fraud has frequently involved financial and telecommunications sectors, and often have been initiated through digital platform communication. Firms and individuals in all three of these sectors have the greatest opportunity to serve as the gatekeepers and to establish protections for Canadian consumers.

While fraud losses are often realized in the financial services sector, we have observed that many fraud journeys begin outside the financial sector and that telecommunications and digital platforms are routinely leveraged by fraudsters. These sectors have clear opportunities to reduce or prevent frauds through early interventions, for example, by preventing Caller ID spoofing or detecting and disrupting fraudulent solicitations through digital platforms. Other potential sectors that could be considered for future phases of the framework include credit card providers, Interac, crypto-trading platforms, and other payment intermediaries.

Addressing the challenge of widespread consumer fraud in Canada will require the coordinated efforts of multiple gatekeepers across the three identified sectors. While no intervention will be 100% effective in combatting fraud, with each sector using its unique position and tools to prevent, detect and disrupt some frauds, collectively these actions hold significant promise to help protect Canadian consumers from falling victim to frauds.

2. What role could a central regulator play in a Multi-Sector Anti-Fraud Framework?

OBSI supports the creation of a strong central body to coordinate anti-fraud efforts across sectors and to consolidate information-gathering and sharing. A central body could:

- establish shared definitions for different types of fraud and consumer harm to help ensure effective communication and data gathering
- develop consistent reporting requirements

- aggregate data from multiple sectors and analyze it to identify trends, emerging threats and prevention opportunities
- establish complementary expectations for each sector based on the most up-to-date and emerging fraud threats and work with sector-specific regulators to track compliance with these expectations
- play a coordinating role during major fraud incidents
- support secure and structured information-sharing among sector-specific regulators and law enforcement, so that organizations can use reliable indicators and system-wide insights to prevent, identify, and disrupt frauds

3. What role could sector-specific regulators play in the Framework?

Sector-specific regulators are best positioned to translate Framework expectations into clear, operational guidelines or requirements tailored to the products, channels, and risks in their respective sectors. These regulators are best positioned to supervise compliance through existing tools (e.g., guidance, compliance examinations, and enforcement).

Consistent sector-level expectations are important to reduce variability in firm practices and outcomes, which consumers could experience as unfairness if they are exposed to varying levels of protection from fraud depending on where a transaction occurs.

4. How can effective oversight of the Framework be achieved, without duplication of existing oversight of the three sectors?

It is important to acknowledge that there is currently very little oversight of fraud-specific market conduct in any of the sectors that will be subject to the new Framework. This presents an opportunity for the new regulator to work collaboratively with existing regulators to develop a coherent fraud detection, prevention and disruption framework for the benefit of all Canadians and reduces the risk of duplication.

Effective oversight of anti-fraud activities in the three sectors can be achieved by distinguishing between strategy development, standard setting and coordination activities, which should be the jurisdiction of the new regulator and sector-specific supervision and enforcement, which should be the jurisdiction of existing regulators. While some duplication of effort may be inevitable, from a consumer protection perspective, avoiding gaps in accountability, particularly for frauds that utilize multiple sectors, is more important than minimizing administrative overlap.

5. When should Framework regulators be permitted to share fraud-related information with each other to further the Strategy aims of preventing, detecting, disrupting, and investigating fraud?

Given the overarching purpose of the Framework and the vital importance of combatting fraud in Canada, an expansive and open approach to information sharing is justified. While personal information should always be safeguarded and all participants in the Framework should be collectively subject to appropriate data protection requirements, open information sharing among Framework participants would be beneficial to the overall goals of the initiative.

Openly shared information would assist regulators with identifying active scam campaigns/activities, patterns that affect more than one sector, a systemic breakdown in a firm's or sector's fraud and consumer protection controls, or new fraud methods that are likely to spread quickly. The new anti-fraud regulator should establish protocols for this information sharing and may serve as a central repository for shared information.

In the context of a broad authority to share information for the purposes of the Framework, more focus could be brought to identifying those circumstances where the sharing of information should be prohibited.

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?

Regulators should share practical information that helps identify and stop fraud. This could include fraud types and trends, weaknesses in firm controls and specific warning signs, such as confirmed scam websites or phone numbers, and known networks or patterns.

Information should be shared when there is evidence of active or emerging fraud patterns affecting more than a firm or sector, or repeated failures in controls that are allowing fraud to continue.

The purpose should be as previously outlined in the strategy – to prevent fraud, improve detection, disrupt active scams, reduce consumer harm.

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

While we are supportive of broad information sharing among regulators, in our experience, personal information is often not relevant to the purposes outlined above and should not be included unless necessary.

Directly identifying personal information about fraud victims or consumers more generally should be shared only on an exceptional basis where it is strictly necessary to prevent imminent harm or support an investigation, and only for the precise purposes of prevention, detection, disruption, and investigation.

A clear exception to this is in the identification of known or suspected fraudulent actors. Clearly, the sharing of these identities is relevant to the prevention and disruption of frauds and it should be permitted, however, it also presents the risk of severe harm to any person or entity that is wrongly identified as a fraudulent actor or facilitator. The consequences of a wrongful identification as a fraudulent actor could include the freezing of accounts, the loss of funds in transit, and a broad disruption of all financial interactions, causing potentially significant monetary harm. For this reason, there should be a clear process available to all identified individuals or entities to challenge and reverse any such identification and restore their previously available financial services.

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?

Response to Questions 8-11

Our views on information sharing between law enforcement organizations and framework regulators are similar to those outlined above in relation to information sharing between regulators. In general, our observation is that greater information sharing is supportive of and consistent with the overarching goals of the Framework, subject to limitations around the sharing of personal information and caution about the potentially negative consequences of inaccurate identification of an individual or entity as a fraud actor. Any such sharing should be managed in a way to prevent unintended harm, and it should include safeguards so consumers have recourse or can challenge decisions that rely on shared information.

We also note that, from a consumer harm perspective, referral to law enforcement should not substitute for or delay active steps to protect consumers by organizations (e.g., transaction holds, warnings, or recall attempts).

Similarly, sharing of information with private sector organizations, whether by law enforcement agencies or the Framework regulator, offers the promise of potentially significantly disrupting and preventing active frauds, but also presents the risk of serious harm to anyone wrongfully identified. In our experience, financial institutions are highly risk-averse and likely to refuse to offer services to anyone that they perceive as potentially involved in a crime or wrongdoing, which can lead to significant harm to the impacted individual. As described above, identified individuals should be informed that they have been identified and given the opportunity to respond and/or disapprove the allegations against them.

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

There are many ways for organizations to embed Framework compliance within their governance models, including board-level oversight, clearly assigned executive accountability, documented fraud risk assessments, control testing and assurance; escalation protocols, and post-incident remediation with lessons learned.

13. How can organizations ensure that anti-fraud training is effective, and how should this be reflected in government policy or legislation?

Empowering frontline staff to act when there are signs that a consumer may be at risk of fraud is critically important. Staff in branches and call centres are often best placed to recognize common fraud patterns, warn consumers in real time, and take immediate steps to prevent further harm, including placing temporary freezes where appropriate. To support this role, consideration should be given to safe-harbour protections that allow staff to take good-faith action to protect consumers, without fear of negative consequences to themselves or their institution.

Anti-fraud training should be role-based, scenario-driven, continuously updated, and assessed for competence rather than attendance. Fraud training should be specific to the role. Training should be refreshed as fraud typologies evolve and should include frontline staff, fraud operations, complaint handlers, and leadership. The Framework regulator could require periodic validation of training effectiveness, using both testing and outcome measures.

14. When and how should organizations be required to validate the identity of users of their services?

Organizations should be required to validate identity before processing account changes, receiving instructions, and disclosing information. Identification practices that are more easily exploited by fraudsters include SMS-based two-factor authentication and over reliance on basic personal information, which might be widely available due to data breaches and online exposure. In our experience, stronger identification methods include biometric identification, unique user information, such as IP addresses and behavioral patterns, and the use of information that is difficult for fraudsters to obtain or guess, such as details from recent account activity (for example, the last payment made).

Organizations should adopt a risk-based approach to identity validation, with stronger verification methods for higher-risk actions, such as account recovery, changes to credentials or contact details, addition of new payees, and unusually large or atypical transfers. In many fraud complaints, compromise occurs at these critical points. Clear expectations around identity validation also help define whether reasonable steps were taken when losses occur.

15. What fraud-related information should organizations be required to make available to individuals using or who may use their services?

Clear and easy-to-understand fraud information should be accessible to consumers, especially at key moments before sending money. This includes clear warnings for higher-risk transactions, explanations of common scams, steps consumers should take to keep records, and straightforward information on how to report suspected fraud and what will happen next. Based on our experience, general warnings posted on websites or sent by unsolicited emails or hidden in contracts are unlikely to influence people’s actions and do not meet consumer expectations for real protection.

16. How should the effectiveness of organizations' fraud education be assessed to ensure it meaningfully reduces harm?

Effectiveness could be measured by analyses of reported fraud data, such as reductions in repeated victimization, lower avoidable losses from common or serious scams, and evidence of improved consumer understanding through testing or surveys. Complaint patterns, especially consistent confusion about protections and how processes work, should also be part of the assessment. OBSI supports sharing education results with regulators so programs can be improved based on evidence rather than assumptions.

17. What sector-specific fraud-prevention rules should be in place?

Financial Service Sector

In our response to the Department of Finance Consultation on Proposals to Strengthen Canada's Financial Sector in September 2024, we outlined in considerable detail our experience and views on three highly interrelated potential policy initiatives for addressing fraud in the financial service sector. The themes of that commentary included:

- Requiring banks to detect fraud
- Requiring banks to delay or prevent transactions
- Establishing a limited liability system for bank fraud, essentially shifting liability for fraudulent transactions from consumers to banks

Our views on these important public policy initiatives remain unchanged. We note that some policy interventions discussed in the 2024 consultation were implemented as a part of Budget 2025.

Telecommunications sector

In many of the fraud cases that we see at OBSI, telecommunications networks and equipment are an important part of the communication between the criminal and the victim, and in some cases, lend credibility or the appearance of authenticity to fraudulent schemes. For example, in many cases where the fraud was initiated by telephone, the call display information states that the name and number of the caller are a financial institution. It is our understanding that these calls are often made to many potential victims simultaneously or near simultaneously.

Our experience leads us to believe that telecommunications system operators have the opportunity to perform a vital gatekeeping role in Canada's anti-fraud initiatives. For example, by addressing the technological systems that allow for caller ID spoofing, by implementing mechanisms to detect patterns of usage that are typically used by fraudulent actors, and by disrupting access to the telecommunications networks when such fraudulent patterns are detected. Rules should be put in place to require telecommunications sector firms to implement changes and technological interventions to address this potential opportunity to protect Canadians from fraud.

Digital platforms

In our experience, frauds and scams are often initiated through digital platforms. Criminals intending to commit fraud often reach out to their victims through social media platforms, email, and other digital communications channels.

Digital platforms have an opportunity to perform a vital gatekeeping role to detect and prevent frauds at the earliest stages. For example, by identifying messages and promoted content that follow the patterns typical of frauds and scams, by monitoring communications between system users for content consistent with frauds, and by denying access or disrupting the online actions of suspected fraudulent actors. Rules should be put in place to require digital platforms to develop and implement such identification and disruption technologies.

A key consideration for policy makers will be whether to adopt an approach that is highly prescriptive and requires specific interventions or actions to be undertaken by firms in the banking, telecommunications or digital platform sectors, or whether to rely on a principles-based system. While highly specific lists of requirements offer the advantage of clarity and clear enforceability, they are unlikely to remain current or relevant in the fast-changing environment of online fraud. More principles-based approaches are more likely to remain meaningful over time but are less certain and more subject to interpretation by industry participants and regulators.

18. How could organizations be incentivized to effectively detect and investigate potentially fraudulent activity on their services?

Incentives are strongest when expectations are paired with accountability and liability. As we stated in our submission to the Department of Finance in September 2024, OBSI believes that shifting liability for the harms caused by fraud from the victim to service providers in circumstances where there has been no gross negligence on the part of the victim would serve as a powerful incentive to all Framework participants to engage seriously in anti-fraud initiatives.

By shifting liability for fraud to the Framework participants, the institutions will have an immediate financial motivation to develop and implement detection and prevention mechanisms for their customers, and to maintain and update such systems as the fraud environment changes over time.

Therefore, while we support the fraud detection and prevention proposals set out in the consultation document, our overarching view is that a liability-based system is preferrable, or would be complementary to such prescriptive requirements.

Liability for harms to non-negligent fraud victims, and the distribution of liability among framework sector firms, could be made subject to compliance with the specific prevention actions established by the Framework regulator.

19. How should organizations be required to assess fraud-related harms to individuals using their services?

In our experience, fraud related harms can usually be clearly defined in financial terms. The frauds are usually exclusively focused on extracting money from victims, and we typically assess the harms experienced to be equal to the amount lost. Other impacts, such as identity theft, damage to credit, significant time and stress, and a greater risk of being targeted again are important and potentially significant but are more difficult to quantify when working to resolve a fraud complaint. Often, where these non-financial harms appear significant, we will assess an amount of financial compensation to recognize the potential ongoing impacts to the consumer. Ongoing services, such as credit monitoring, can also be a part of a compensation package.

20. What actions should organizations be required to take to assess risk of future harm to individuals impacted by fraud?

Organizations should be required to take practical steps to lower the risk of repeated victimization. This includes resetting passwords or credentials, enhanced monitoring, targeted warnings, checking payees and contact details, and providing clear guidance on restoring identity. OBSI has seen cases where people were victimized repeatedly when known vulnerabilities were not addressed. Clear expectations for follow-up support after a fraud incident would help prevent future losses and strengthen consumer confidence.

21. When should regulated private sector organizations be able to share fraud-related information with each other?

Our views on information sharing between private sector organizations are similar to those outlined above in relation to information sharing between regulators. In general, our observation is that greater information sharing is supportive of and consistent with the overarching goals of the Framework, subject to limitations around the sharing of personal information and caution about the potentially negative consequences of inaccurate identification of an individual or entity as a fraud actor.

Private sector organizations should be encouraged to share fraud-related information when it is necessary to prevent, detect, or disrupt fraud and to support tracking and recovery efforts. This is especially important for active scams and identifying networks used to move stolen money.

As we observe above, sharing of information among private sector organizations offers the promise of potentially significantly disrupting and preventing active frauds, but also presents the risk of serious harm to anyone wrongfully identified. In our experience, financial institutions are highly risk-averse and likely to refuse to offer services to anyone that they perceive as potentially involved in a crime or wrongdoing, which can lead to significant harm to the impacted individual. As noted above, identified individuals should be informed that they have been identified and given the opportunity to respond and/or disapprove the allegations against them.

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?

Information sharing should focus on clear signs and patterns that can help prevent harm. This includes scam websites, phone numbers, or wallet addresses, signs that accounts are being used to move stolen money, device or behaviour patterns, and information about common scam methods. Information should be shared when it is confirmed or highly reliable, and when the receiving organization can take specific steps to stop further losses or help recover funds.

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

Strong privacy safeguards include clear legal authority, limits on how information can be used, sharing only what is necessary, controlled access, record keeping of use, independent oversight, limits on how long information is kept, and ways to correct errors. Because incorrect information can seriously harm consumers, it is essential to have strong governance over shared lists, including clear processes to review, update, and remove information when needed.

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?

Response to Questions 24-29

Please see our response above to questions 8-11 and 21-23 in relation to information sharing between regulators and law enforcement, and information sharing among private sector organizations. Our general observations, recommendations and cautions apply equally to information sharing between law enforcement, government, and private sector organizations.

30. What sector-specific fraud detection rules should be in place?

All sectors have an important role to play in detecting and preventing frauds and should be required to undertake the gatekeeping functions appropriate to their role in the consumer services landscape. The rules in place for each sector should require industry participants to take appropriate measures to identify unusual transaction activity, signs that accounts have been taken over, and patterns linked to fraudulent activity and moving stolen money. There should also be clear expectations for how quickly organizations step in once warning signs appear.

For digital platforms and telecommunications services providers, using algorithmic and AI tools to identify patterns of communication associated with potential fraud and disrupting those communications is crucially important. These platforms are also uniquely placed to deliver timely warnings to system users when potential fraud is detected.

For the banking sector, as we observed in our September 2024 submission, fraud detection is foundational to any prevention strategy. Canadian banks, like banks around the world, have invested significantly in policies and systems to detect fraud and scams, including customer verification systems, real-time transaction monitoring and regular employee training. However, as we have seen, the systems and processes currently in place have not been sufficient to prevent frauds and scams from seriously impacting Canadian consumers. We have observed many cases where fraud detection systems have failed to protect consumers and where the application of the systems and processes has been inconsistent and inadequate.

We have also observed significant differences in the approach that each bank takes to fraud detection, prevention and remediation. In the absence of any regulatory fraud detection requirements, each institution determines its own security posture and the priority and investment it chooses to make on behalf of its customers. Bank consumers, however, have no way to assess the quality of a bank's fraud detection program and therefore cannot choose their bank on this basis, so traditional market forces cannot be relied upon to motivate banks to invest in robust fraud detection technologies.

We believe there is an opportunity for Canadian banks to invest in developing improved monitoring and detection systems, including those that analyse consumer behaviour and detect patterns of fraudulent transactions in a more accurate and consistent manner and that this is an appropriate area for regulatory standards to be established.

As described in our 2024 response letter, based on our experience, the circumstances where detection could be required for banking industry participants include:

- Consumers report potential fraud or express concerns about one or more transactions or alerts
- Patterns that suggest potential fraud, such as the following circumstances, especially in combination:
    - Unusual transactions that deviate from the customer's normal behavior, such as:
        - New types of transaction for the consumer where they have never used the banking service or product that is being used to initiate the transaction
        - A transfer amount much higher than typical for the consumer
        - Unusual frequency and/or numbers of transfers

        - Transfers at a time of the day that is not normal for the consumer, for example between 1-5 am local time
        - Transfers to a recipient in a geographic location where the consumer has no prior connection
        - Logins from an unusual IP address, especially one that is geographically distant from the consumer's normal location
    - Transactions that match known patterns of fraudulent activity, such as receipt of multiple e-transfers followed by immediate e-transfers out of the account
    - Transfers to a new payee or payees
    - Transactions linked to individuals or accounts previously involved in frauds or scams
    - Multiple transfers slightly below or at the daily limit
    - Transfers to higher-risk recipients, including payment sites like Wise/Western Union or online gambling, unlicensed crypto sites and adult sites, especially where consumer has no history of prior transfers
    - Multiple logins from geographically distant locations in a short period of time
    - Transfers initiated through a newly added or rarely used device
    - Intra-account transfers before an e-transfer, e.g. from a line of credit or credit card to a chequing/savings account immediately prior to the e-transfers
    - Unusual account changes or attempted account changes, for example changing any core information (password, phone number, email address, method of OTP delivery) immediately before a large e-transfer or many small ones in quick succession adding up to a large amount
    - Failed logins or change password attempts shortly before a transfer request
- Consumers are vulnerable or at higher risk of fraud, for example where:
    - the consumer has no technology presence – i.e. no online banking profile, no computer, no email or other enabling technology
    - the consumer is a senior
    - the account is being controlled through a power of attorney
    - the consumer is a previous fraud victim
- Unusual telephone banking interactions – for example, where a purported consumer calls the bank and can't answer verification questions or is trying to circumvent normal procedures by claiming no access to text messages and/or refuses OTP verification
- Transactions that exceed an established daily limit
- Daily limit increases immediately before transfers
- Any failure to accurately respond to verification text messages or phone calls

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?

While fraud detection and prevention measures are likely to introduce frictions and delays for financial services consumers, a degree of inconvenience is justifiable given the potentially devastating consequences of fraud.

If all industry participants are held to the same detection and prevention standards, we would expect industry participants to invest in developing innovative mechanisms to offer these protections while competing for market share and offering services at an acceptable level for consumers. Each service provider would likely establish interventions that balance their regulatory compliance requirements and consumer protection with the attractiveness and usability of their service offerings. We would expect this to involve less intrusive safeguards in lower-risk situations and extra safeguards in higher-risk situations.

To protect legitimate users, service providers could use mechanisms such as prompt notifications, clear explanations of any restrictions, and straightforward opportunities for consumers to restore services where appropriate, with additional care for people who may be more vulnerable.

Importantly, if consumers have opted to turn off access to particular banking products and services, especially any feature that can transfer funds out of an account, reactivating such a feature should not be possible except with additional validation tools such as an in-person authorization.

32. In what situations should regulated entities be required to pause potentially fraudulent activity?

Organizations should be required to pause transactions anytime that signs of fraud, such as those described above in response to question 30, are detected. To avoid unnecessary interruptions of service, exceptions could be permitted, for example, minimum monetary limits. Policy makers could give consideration to establishing a framework where pauses are required in some circumstances and permissible in other circumstances. For example, pauses could be required where there is a high risk of scam or fraudulent activity and where a pause is likely to prevent irreversible loss, and pauses could be permissible in lower-risk scenarios.

33. What measures, safeguards and recourse should be put in place to ensure that individuals' access is not improperly suspended or removed?

Fraud-prevention measures should be fair, transparent, and reversible. When prevention measures are taken, consumers should be notified promptly with a general explanation of why action was taken and information about how they can restore services and/or escalate concerns. If access is wrongly limited, organizations should restore it quickly and provide appropriate remedies, along with clear options for escalating complaints.

34. How can notifications of suspected fraudulent activity be effective?

Notifications are most effective when they are timely and actionable. OBSI supports requiring notifications to clearly warn consumers of any risks detected to be sent at the earliest possible opportunity, ideally while the consumer may still be able to stop or change the transaction. Using more than one communication channel is essential, particularly where one communication channel may be compromised by the fraudulent actor. Notifications should be expressed in plain, simple language and set out clear next steps that the consumer can take to address the problem, for example, “reply STOP to freeze this account”.

35. What sector-specific fraud disruption rules should be in place?

Similarly to our response to question 32 above in relation to pausing of transactions, organizations should be required to disrupt transactions anytime that signs of fraud, such as those described above in response to question 30, are detected. To avoid unnecessary interruptions of service, exceptions could be permitted, for example, minimum monetary limits.

Policy makers could also give consideration to establishing a framework where disruption is required in some circumstances and permissible in other circumstances. For example, disruption could be required for high-value transactions or where there is a high degree of certainty that a scam or fraudulent activity is occurring and the disruption is likely to prevent irreversible loss, while disruption could be permissible in lower-value and/or lower-certainty scenarios.

Clear, sector-specific rules that set basic expectations for how organizations should disrupt fraud in higher-risk situations should be in place. This could include rules that stipulate:

- required or expected communication or transaction pauses when warning signs are detected
- immediate action to freeze, recover or trace funds
- requirements for cooperation between organizations within and across sectors to stop active scams

Considerations should also be given to the consequences imposed on organizations for failure to disrupt frauds and scams in accordance with the rules. Imposing financial responsibility for such failures will help ensure organizations invest in the ability to act quickly and consistently.

Consumers should also be empowered with tools that they can use to disrupt frauds or scams if they suspect that their account may have been compromised, or in response to warning notifications that they have received. Such tools should include the ability to freeze accounts or certain capabilities of the account, for example, the ability to freeze all transfers out of the account.

36. How should organizations be required to make it easy for users to report fraud activity to them?

Organizations should offer easy and accessible ways for consumers to report fraud, such as through an app, website, or by phone. Consumers should have the ability to immediately lock their accounts or account capabilities and should be asked to provide any evidence that may be relevant to the detection or prevention of similar frauds in other accounts. Consumers who report suspicions of fraud should receive timely confirmation that their report was received. They should also receive a clear explanation of what will happen next and how long it may take, with added support for vulnerable individuals. Based on our experience, inefficient intake processes, long wait times, staff training deficiencies, and difficult or lengthy customer authentication procedures can significantly undermine timely disruption of fraudulent activity, investigation and resolution.

37. How could organizations effectively investigate cross-sector complaints?

Effectively investigating complaints involving multiple firms, especially firms in different sectors, is likely to be very difficult. In our experience, complaints involving multiple firms are typically investigated in a siloed manner by each firm involved. Sometimes, this is sufficient and the firm at fault for the error recognizes its responsibility and appropriately addresses the complaint. Often, however, where the responsibility is shared or unclear, neither firm accepts responsibility or makes their acceptance of responsibility conditional on the other firm's acceptance.

Ideally, organizations involved in the same fraudulent incident would work together to share information and responsibility where appropriate. Realistically, however, where multiple firms or sectors are involved, fragmented investigations and self-interest are likely to severely diminish the timely investigation and fair resolution of the complaint, leaving consumers to manage multiple, unproductive complaint handling procedures simultaneously. To avoid this outcome may require the involvement of an independent third party, who could serve as a central coordinator of the complaint and facilitate fair, shared resolutions where appropriate. For example, the independent third party could perform the following functions:

- receive the complaint from the consumer and clarify the allegations against all industry participants involved
- communicate the complaint to all industry participants
- receive the investigation findings from all industry participants, working with them to clarify any inconsistencies
- determine a fair allocation of responsibility if multiple industry participants share fault
- coordinate communication of investigation findings and settlement recommendations with the consumer

38. How long should organizations have to internally investigate complaints?

Today, federally regulated banks have up to 56 days to investigate and resolve complaints internally before consumers can escalate their case to OBSI. This timeframe has proven workable in practice and gives consumers a clear right to escalate when internal processes are not completed in a timely manner or are otherwise unsatisfactory.

As many complaints under the Framework are likely to involve banks, it would be appropriate for investigation timelines under the Framework to match the Bank Act timelines. Having one coordinated investigation timeline for all regulated organizations would be logical, straightforward to communicate, and appropriate in the circumstances.

39. What information should organizations be required to include in a summary of complaint?

Complaint closing summaries should contain clear, complete, and standardized information that allows the consumer, the organization, regulators, and any external complaints body to understand the nature of the dispute, what has been reviewed, and the reasons for any resolution offered. The summary should also provide consumers with information about the next steps that they can take to escalate their complaints if they are not satisfied.

The content of substantive response letters from financial institutions to complainants is prescribed by regulations in the securities and banking sectors. There is a reasonable consensus on best practices for these letters.

For example, Canadian Investment Regulatory Organization (CIRO) Rule 3756, which has been recently updated and is currently in the final stages of its public consultation process, proposes the following requirements:

- Substantive response letters must be sent to each complainant.
- The substantive response letter must be written in plain language and be in a format readily accessible and understandable by the complainant.
- The substantive response letter must include the following information:
    - a summary of the complaint,
    - the result of the firm's investigation,
    - the firm's decision on the complaint, including an explanation of the factors that led to the decision,
    - a statement describing to the consumer the options available if the consumer is not satisfied with the firm's response, including the availability of the approved ombudsman service and any time restrictions for escalations that may apply
    - A statement that the consumer may submit a complaint to the regulator for an assessment of whether any disciplinary action is warranted

Similarly, the Financial Consumer Agency of Canada outlines the prescribed content for substantive response letters in its publication *Guideline on Complaint Handling Procedures* (published in 2022 and currently under review). The guideline includes the following requirements in Section 48:

- The substantive written response should provide all the information a Consumer needs to make an informed decision on whether to submit the complaint to a Bank's external complaints body, if they so choose, including:
    - the date on which the complaint was communicated to the Bank
    - the fact that the prescribed period has been reached and that the Bank was unable to Resolve the complaint within that period, if applicable
    - a statement of facts relating to the complaint
    - the Bank's final decision and offer, if any, in response to the complaint, as well as any relevant information about how the final decision was reached
    - the method used to calculate redress (monetary or non-monetary), if applicable
    - the Consumer's right to submit the complaint to the external complaints body and how to contact that body

OBSI has published guidance for firms, entitled *Establishing and Communicating Your Complaints-handling Process*, which includes guidance that firms' final response letters should include:

- A description of the complaint
- The results of the firm's investigation

- A rationale for the decision
- A final paragraph explaining the availability of OBSI in the following terms: "If you remain unsatisfied with our response, you can forward your complaint to the Ombudsman for Banking Services and Investments (OBSI). OBSI is an independent dispute-resolution service that investigates unresolved disputes at no charge to you. An alternative to the legal system, it may recommend compensation up to $350,000. OBSI can be reached at 1-888-451-4519 or www.obsi.ca, and must be contacted within 180 days of receiving this final response to your complaint."

40. Should organizations be held liable when they do not fulfill their obligations under the Framework?

As we stated in our response to question 18 referencing our submission to the Department of Finance in September 2024, OBSI believes that shifting liability for the harms caused by fraud from the victim to service providers in circumstances where there has been no gross negligence on the part of the victim would serve as a powerful incentive to all Framework participants to engage seriously in anti-fraud initiatives.

By shifting liability for fraud to the Framework participants, the institutions will have an immediate financial motivation to develop and implement detection and prevention mechanisms for their customers, and to maintain and update such systems as the fraud environment changes over time.

Liability for harms to non-negligent fraud victims, and the distribution of liability among framework sector firms, could be made subject to compliance with the specific prevention actions established by the Framework regulator.

41. What standards should apply in determining whether an organization fulfilled its obligations?

In establishing standards and evaluating whether an organization fulfilled its obligations, the following factors are particularly relevant:

- Whether appropriate controls were in place and operating effectively, including authentication measures, transaction monitoring, and fraud-detection tools proportionate to the risk profile of the activity.

- Whether the organization responded promptly once risk indicators were triggered, including applying protective measures such as warnings, enhanced verification, temporary blocks or holds, recalls, or transaction reversals where feasible.

- Whether actions were taken in time to prevent or limit harm, recognizing that delays can materially reduce the likelihood of recovering funds in fraud cases.

- Whether communications with the consumer were timely, clear, and actionable, including warnings, explanations of risk, and guidance on next steps.

- Whether complaint handling and investigation processes met applicable service standards, including cooperation with other parties where required and preservation of relevant evidence.

42. How should liability be apportioned when multiple organizations have not fulfilled their obligations?

Liability should be apportioned based on each organization's degree of control over the relevant risk point and contribution to the failure (e.g., identity/authentication gaps, monitoring failures, failure to act on indicators, delayed recovery steps, or lack of cooperation). To protect consumers, policymakers should avoid models that leave individuals uncompensated while institutions dispute fault. A consumer-first approach -- where redress occurs promptly and allocation is resolved between organizations afterwards -- can reduce delay and improve fairness.

From a practical perspective, apportionment of liability among service providers is likely to be contentious and difficult for service providers to resolve without clear guidance and/or external supervision. Such apportionment could be based on a presumption of equal sharing of responsibility, with an onus on service providers who believe they have less responsibility to prove that a different apportionment would be fair. The Framework regulator could assume oversight of unresolved apportionment disputes, or this responsibility could be delegated to the external complaints body.

43. What should inform how an external complaint body is chosen?

As a preliminary matter, a priority should be placed on ensuring that consumers have access to an independent, accessible ombudservice for unresolved complaints arising under the proposed Framework.

As outlined in our October 2021 submission to the Department of Finance's consultation on Strengthening Canada's External Complaint Handling System, access to a fair, effective and trusted ombudsman service is recognized internationally as a vital component of a country's financial consumer protection framework because:

- It provides access to justice for consumers who find themselves in a dispute with their financial services provider
- It meets consumers' expectations of fair treatment and supports consumer confidence in the financial services sector
- It encourages effective firm-level complaint handling
- It provides information to regulators, industry participants and the public about challenging consumer experiences that feeds into a virtuous cycle of systemic improvement

Additionally, the ECB structure for the proposed Framework that would best meet the needs of Canadians is a single financial ombudsman service and that is mandated and accountable to the Framework regulator. In our 2021 submission, we also described in detail the reasons why competition between ECBs is not in the public interest and raises a reasonable apprehension of bias. There are five key problems with ECB competition:

- Consumer confusion

- Real and perceived systemic bias towards the financial services providers who choose the ombudsman
- Gaps for cases that involve multiple institutions
- Diminished informational value of disaggregated data
- Reduced efficiency of scale and scope

The selection of an external complaint body for complaints arising under the Framework should be informed primarily by whether the body has the structure, experience, and capability to resolve a high volume of complaints involving potentially significant financial harm. In particular, consideration should be given to whether the body:

- Is constituted specifically to resolve financial consumer disputes, including complaints involving disputed responsibility, financial loss, and compensation.

- Has experience operating within a clear statutory and regulatory framework, with defined accountability obligations, including reporting requirements, service standards, and independent review mechanisms.

- Demonstrates independence and impartiality, supported by governance arrangements that protect decision-making from influence by participating firms and ensure fair processes and outcomes.

- Has the expertise and investigative capacity to assess complaints involving complex financial products, internal controls, authentication processes, and consumer-protection obligations, including where issues such as fraud or unauthorized transactions are alleged.

- Provides accessible, transparent, and consistent processes at no charge to consumers, including assistance throughout the complaint process and clear communication of findings and outcomes in both official languages.

- Produces timely, reasoned outcomes, including compensation recommendations where appropriate, supported by established methodologies and publicly reported performance metrics.

- Is positioned to identify and escalate systemic issues, so that trends in complaints can inform regulators' supervisory and policy work.

44. Should decisions of the external complaint body be binding?

In our view, empowering the ECB for the proposed framework to make binding decisions would be ideal, but it is not necessary to realize many of the benefits of the ECB system.

In the thirty years that OBSI has been working with banks and their customers to resolve disputes, banks have almost always offered to resolve consumer disputes in accordance with our recommendations. This is in contrast to our experience with securities firms. With respect to our securities mandate, OBSI has long

sought greater powers to secure redress, chiefly because the current system of "name and shame" gives firms the ability to act on the economic incentive they have to offer to settle complaints below (sometimes far below) the compensation amounts that we consider fair in all the circumstances of the case, and leaves consumers with no realistic option but to accept such settlements. The practice of name and shame, when it does occur, can also unfairly tarnish public perception of the industry as a whole. This challenge has been observed consistently over time and has been noted by independent reviewers, consumer advocates, and securities regulators.

While we have not experienced similar challenges with banks - and are generally of the view that the current system of name and shame is effective in allowing us to reach fair resolutions in disputes between banks and their customers - we are aware of the public perception of our non-binding mandate as less effectual or weaker than a binding mandate. It is not uncommon for our non-binding mandate to be referred to as "toothless".

Because of the importance of this issue from the perspective of public perception, we would recommend a binding mandate for framework disputes, though in our view the ECB would likely also be able to achieve fair dispute resolution for disputes under the proposed framework with non-binding powers.

45. How long should the external complaints body have to investigate escalated complaints?

We believe that all stakeholders benefit from a dispute resolution process that reaches fair conclusions as efficiently as possible. The amount of time a case requires to resolve depends on many factors, including the subject matter of the complaint, the available evidence, case complexity and the availability or participation of the firm and consumer.

Under the Bank Act, OBSI is required to resolve all banking complaints -- including fraud complaints -- within a maximum of 120 days. Based on OBSI's experience investigating complaints, most banking-related cases are completed within 60 days, almost all are resolved within 90 days, and some highly complex cases require up to 120 days.

We believe it would be appropriate for the complaint resolution time limits under the framework to match those in the Bank Act. This would ensure adequate time for the ECB to complete its work and would allow for straightforward communication of timelines to interested stakeholders.

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

The Canadian public benefits from the fraud awareness efforts of many key stakeholders, including the Government of Canada. The FCAC in particular has done considerable excellent work in this area, as has the Canadian Anti-Fraud Centre, Canadian securities regulators, traditional media journalists, and others. This public messaging has undoubtedly increased Canadians' awareness of fraud generally but clearly has not been sufficient to fully empower Canadians to protect themselves.

Modern technology offers some intriguing new avenues for public education in this area, including the facilitation of highly targeted information and message delivery at key points in consumers' decision-

making processes. Financial institutions, telecommunications companies and digital platforms are themselves particularly well placed to deliver highly targeted warnings and key messages to consumers at critical decision points.

47. How can the government improve Canadians' awareness about the risk of misuse of government-issued identifiers, including social insurance numbers?

Government can improve awareness through plain-language guidance on when identifiers such as SINs are legitimately required, how scammers misuse them, and the immediate steps consumers should take if compromise is suspected. In addition, limiting unnecessary collection of identifiers and promoting practical recovery tools (e.g., credit alerts and reporting pathways) can reduce harm. Any approach should be accessible and tailored to varying levels of consumer digital literacy.

48. What can be done to support federal law enforcement's ability to investigate fraud and collect fraud-related intelligence?

We do not have any comments in response to this question.

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?

We do not have any comments in response to this question.

50. What role should the CAFC play in advancing the Strategy?

We do not have any comments in response to this question.

Thank you for providing us with the opportunity to participate in this important consultation. We would be pleased to provide further feedback to the Department of Finance at any time.

Sincerely,

Sarah P. Bradley
Ombudsman & CEO