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

September 11, 2024

Delivered by email to: legreview-examenleg@fin.gc.ca

Director General
Financial Institutions Division
Financial Sector Policy Branch
Department of Finance Canada
90 Elgin St
Ottawa ON K1A 0G5

Re: Response to request for comments on Proposals to Strengthen Canada's Financial Sector

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, *Proposals to Strengthen Canada's Financial Sector* (the "Consultation Document").

OBSI is a national, independent, and not-for-profit organization that helps resolve and reduce disputes between consumers and over 1500 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 27 years. As such, we are uniquely positioned to share our views and insights for this important consultation.

As long-time advocates for a fair, effective and trusted financial services sector, we support the overarching goal of this consultation, particularly its timely focus on consumer protection and how to better protect Canadians consumers and businesses from fraud. Improved systems for fraud detection and prevention are important consumer protection initiatives that will enhance consumer confidence in Canada's banking system as well as the fairness, stability and prosperity of the Canadian financial services sector as a whole.

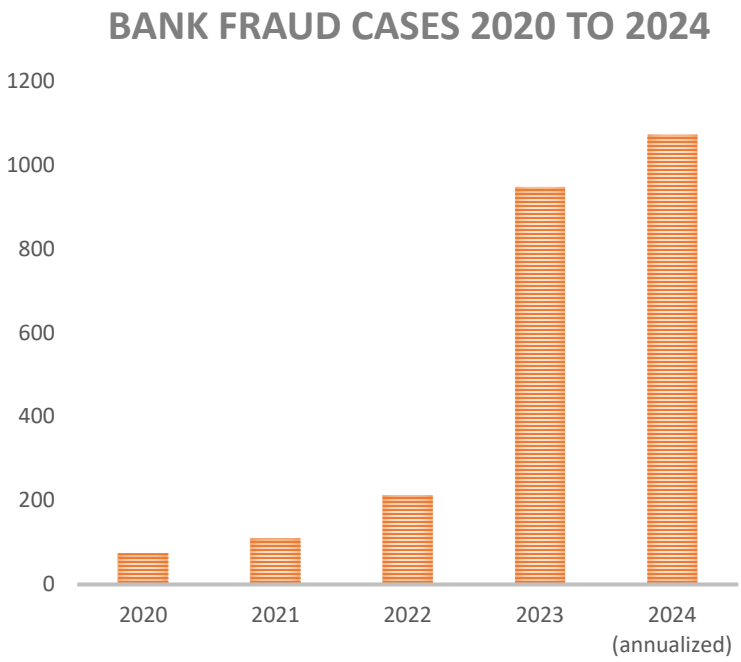
OBSI's experience with bank fraud

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

In 2021, OBSI opened 110 cases related to bank fraud. By 2022, this number had nearly doubled to 213 cases. In 2023, we opened 946 fraud related cases – a 350% year-over-year increase, and this year, we

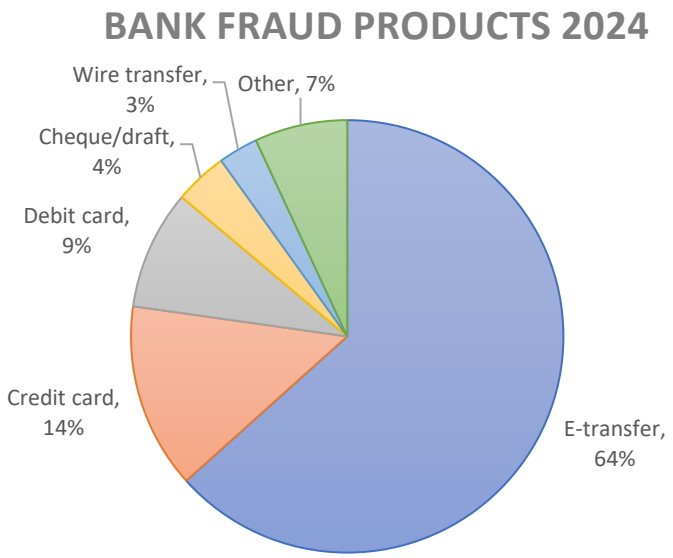
are on track to open approximately 1160 cases. Of the banking fraud cases we have opened in 2024, 68% relate to e-transfers (including global money transfers), 12% to credit cards and 8% to debit cards.

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. 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.



In many of these cases, the consumer admits, or the bank's records indicate, that the consumer has unknowingly shared their confidential banking information (card number, passcodes and/or two-factor authentication number) with a criminal. Consumers share this information either by being tricked into doing so (e.g. by a criminal pretending to be a bank employee) or by inadvertently giving a criminal access to their device (e.g. by clicking on a criminal's link that appeared to be legitimate).

In 2023 approximately one in five fraud cases resulted in a settlement or recommendation for compensation to the consumer. In most cases we are not able to recommend compensation because we have no legal or regulatory basis to do so. Sharing confidential banking information, intentionally or unintentionally, is a breach of the agreement that consumers make when opening a bank account, leaving them liable for their losses in most fraud cases. Banks have limited obligations to protect their customers from these crimes. When we do recommend compensation in fraud cases, it is usually because we have determined that the bank has not met its obligations under the *Canadian Code of Practice for Consumer Debit Card Services* (the Debit Card Code) or the *Code of Conduct for the Delivery of Banking Services to*



Seniors (the Seniors' Code), has not lived up to its own public representations about fraud detection and prevention, or has failed to prevent a specific fraud when it had a clear opportunity to do so.

We note that for e-transfers, there are currently no specific laws or regulations in place outlining the obligations of consumers or banks. As a result, the obligations between the two parties are based on the bank's account agreement, with each bank having its own agreement with different accountabilities, including the bank's expectations of consumers to protect their information, and no maximum liability applied. When banks do provide restitution, they often do so as a goodwill gesture.

In our experience, consumers often incorrectly believe that they are protected from fraud and that their bank will return any money they have lost to fraud. This consumer expectation is likely based on the general understanding and advertising of "zero liability" protections for credit card products, banks' public representations about security and fraud protection, and the general reputation of banks as safe, secure places for the safekeeping of consumer deposits.

Because money is generally not recoverable once transferred to criminals, prevention of fraudulent transfers, through consumer education, enhanced detection mechanisms, improved bank product design, improved law enforcement, and cooperation among the service providers whose infrastructure is used to facilitate bank fraud, is essential to reducing the harm caused by these crimes and preserving the confidence of the general public in Canada's banks.

Example 1 - A common e-transfer fraud case

Mr. E held personal chequing and savings accounts at his bank. He found online banking on his laptop and cell phone convenient and frequently accessed his accounts through his bank's mobile application. His bank sent him e-mail notifications about his account activity, and he often confirmed his account balances online. He protected his devices with passwords and kept them confidential.

One day, Mr. E received a notification from his bank that his chequing account balance was low. He logged into his account to investigate and found nothing unusual. Shortly afterward, however, he received another notification confirming two e-transfers from his account. He did not recognize the transactions, so he logged into his account again via online banking and discovered that two e-transfers for $3,000 each had been sent from his account.

The cost of consumer protection

We note that all of the proposals included in the Consultation Document will have significant financial implications for Canada's federally regulated financial institutions. Enhanced fraud detection and prevention mechanisms are costly and complex undertakings for any institution and any liability regime will also come at a significant financial cost to the institutions that are required to indemnify their customers for unauthorized transactions.

It is important to consider, however, that these costs will ultimately be passed on to the consumers for whom the protections are being implemented through various charges and fees. Some measures will impose indirect costs by causing transaction delays and other inconveniences and frictions. In this manner, the cost of any legislated consumer protection measures will be spread among all consumers, and the task of policymakers is to determine the appropriate level of protection and cost that is justified by the harms they are seeking to prevent.

Consultation questions

Our comments below respond directly to the specific questions in the Consultation Document. While there are important and potentially impactful proposals throughout the Consultation Document, in our submission, we focus primarily on the questions posed under Theme 2, *Enhancing Consumer Protections* and Theme 5, *Upholding World Class Regulation*, as these matters fall most squarely in OBSI's areas of expertise.

As a preliminary matter, we note that the questions in Theme 2 include three highly interrelated potential policy initiatives:

- 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

We will address each of the Consultation Document's questions separately below in the order that they were posed, however, as a preliminary matter we observe that the impact of a requirement to delay or prevent potentially fraudulent transactions is entirely dependent on the quality of a bank's fraud detection systems – since a bank can only prevent a transaction that has first been detected accurately. Similarly, a fraud detection system can only reduce the incidence of fraud if it is used to delay or prevent fraudulent transactions. Detection and prevention are two sides of the same coin, and both are requirements of a functional system, so considering each in isolation is somewhat difficult.

A limited liability regime is a system that could be implemented instead of, rather than in combination with, specific fraud detection and prevention requirements. By shifting liability for fraud to financial institutions, 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 in our comments below we voice support for the fraud detection and prevention requirement proposals set out in the consultation document, this support is subject to our overarching view that a liability-based system is preferrable to such prescriptive requirements.

Requirement to delay or prevent transactions

QUESTION 1: SHOULD BANKS BE REQUIRED TO PREVENT OR DELAY TRANSACTIONS THEY BELIEVE TO BE FRAUDULENT AND/OR ASSOCIATED WITH A SCAM, AND IN WHAT CIRCUMSTANCES THEY SHOULD BE REQUIRED TO EXERCISE THIS FUNCTION?

OBSI supports a requirement to have banks delay transactions that they believe may be fraudulent or associated with a scam. As noted above, meaningful implementation of the requirement to delay or prevent transactions relies entirely on the accuracy and reliability of a bank's detection mechanisms, as well as the bank's systems to intervene quickly when such potential frauds have been identified.

Banks currently have automated systems in place to reduce and prevent fraud for their customers, and doing so is clearly important to them from a customer experience perspective. However, we believe that greater fraud prevention opportunities exist than banks are currently employing. For example, in many cases we have observed that bank records show an anomalous pattern of behaviour prior to or during a fraudulent transaction which could have been detected, such as logins from an unusual geographic location, or significant global money transfer by a person who has never sent one before, or multiple large transactions to a new payee within a brief time period.

In some cases, we can see that the bank's fraud detection systems have flagged transactions as suspicious, but the only action taken by the bank is to send a one-time password to the consumer. This type of authentication will not protect a consumer who has lost control of their device or has been tricked by a fraudster.

When we see obviously fraudulent patterns that a bank has failed to act upon, we may recommend compensation on the basis that the bank has failed to meet its public commitments, such as the Debit Card Code, the Seniors' Code, and the bank's own marketing materials relating to its fraud detection technologies. However, in cases

Example 2 – Detection system fails to prevent fraudulent transactions

Ms. F held a chequing account and a line of credit at her bank. One day, she received a phone call from an individual impersonating a representative from her bank who asked her to provide her banking information as well as a one-time verification code. Ms. F provided the requested information to the caller. Following this, Ms. F discovered that two electronic transfers had been completed as well as numerous transactions conducted via a new account that had been established, totalling over $7,400.

Ms. F contacted her bank to dispute the charges and was told that she was liable for the charges as she had disclosed her banking information to a third party. Our investigation showed that the completed transactions happened around the same time as multiple declined transactions, which had alerted the bank's fraud department of a potential issue. Ms. F, however, was never informed of this by her bank.

where there are questionable but not obviously fraudulent patterns, we are unable to recommend compensation because banks are under no obligation to identify these patterns and prevent the transactions.

By taking more measures to actively preventing fraud, banks would maintain and enhance consumer trust and confidence in the financial system. In addition, proactive prevention of fraudulent transactions would reduce the overall incidence of financial crime, making the financial system safer for everyone.

Based on our experience, the circumstances where detection and prevention should be required include circumstances where:

- Customers report potential fraud or express concerns about one or more transactions or alerts
- Patterns that suggest potential fraud are detected, such as the following circumstances, especially in combination:
    - Unusual transactions that deviate from the customer's normal behavior
        - 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

Despite the length and detail of this list, the nature of fraudulent activity is constantly changing and evolving as criminals work to avoid any detection mechanism that have been developed to stop them. The technology banks use to detect fraud must continuously evolve if it is to remain effective. Fortunately, financial institutions in Canada and around the world have a wealth of experience in identifying and preventing fraudulent transactions, especially with respect to credit card products. We would expect that Canadian institutions would be able to draw on this knowledge and expertise to help to prevent fraud with respect to other banking products and accounts.

As discussed above, there is likely to be a very significant cost to these fraud prevention mechanisms and these costs will ultimately be built into the cost of banking products and services for all consumers. In our view, given the utterly devastating consequences of frauds and scams for impacted consumers, the costs for prevention mechanisms, when spread across all bank consumers, is appropriate in the circumstances.

Example 3 – Account credentials phished

Ms. V received a text message on her mobile phone from what seemed to be one of her monthly service providers. The message preview indicated that she had been refunded a credit. For more details, she opened the message and clicked on the link provided. She was then prompted to click on the icon for her bank to continue with the refund process and deposit the amount into her bank account. Her bank account was linked to her line of credit and credit card.

After Ms. V clicked on the icon for her bank, her mobile phone screen glitched for a moment. Her husband advised her to report the incident to her bank as soon as possible and find out if any of their accounts had been compromised. She contacted the bank and the representative assured her there was nothing to worry about. Later that evening, she received a notification to confirm that an e-transfer for $3,000 had been accepted by someone she did not know.

Requirement to turn off account capabilities

QUESTION 2: SHOULD BANKS BE REQUIRED TO ALLOW CONSUMERS TO HAVE THE ABILITY TO TURN OFF OR ADJUST ACCOUNT CAPABILITIES TO PREVENT FRAUD, SUCH AS THE ABILITY TO COMPLETE WIRE TRANSFERS

Consumers should have the ability to modify their digital banking product features independently, especially any feature with the capability to transfer funds out of an account. In our view, ensuring that banking products and services are designed to incorporate such consumer control would significantly reduce consumers' fraud risk by allowing them to activate only those features that they need. Our experience has shown that many consumers are unaware of the full range of capabilities of their online banking services and the associated risks of those services. For example, most Canadian bank customers are able to send up to $50,000 per day internationally through the global money transfer available on their online banking service. We have seen many cases where consumers first learned of this capability only after they have been the victim of a fraud and a criminal had transferred significant amounts from their accounts to international recipients.

We recognize that the ability to easily transfer large sums internationally is an important feature for some Canadian bank customers. However, we question whether this capability is appropriate for many Canadians and whether they would choose to enable it, when considering the significant increase in fraud risk associated with it.

We also recognize that banks are under continuous competitive and commercial pressure to increase the ease of use of their digital consumer experience. However, unless fraud protection is central in the design of new products and services, changes that improve usability may also significantly increase consumers' vulnerability to fraud. For this reason, it is vital that consumer protection measures, including the ability to decline or eliminate product features, need to be prioritized.

Example 4 – Money transferred internationally

Ms. A was a senior citizen of modest means who began online banking during the covid pandemic. She had a small amount in her bank account and had a line of credit for emergencies, which she had never used. One day, she logged into her online banking and saw that her bank account was nearly empty and her line of credit balance was over $20,000.

Her bank told her that in a series of transactions over approximately a week, money had been transferred from her credit line into her bank accounts and then to a recipient in another country using the Global Money Transfer function of her online banking service. The bank said that each of the transactions was authorized by the correct entry of a one-time password that had been sent to her. Ms. A did not recognize these transactions, had never used Global Money Transfer, and didn't know that such transfers were possible.

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. Establishing enhanced identification processes for the reactivation of account features will make transferring out from accounts more difficult for fraudsters. While this will also make such transfers more difficult for consumers, such inconvenience is justifiable given the potentially devastating consequences of fraud.

In addition, informed choice about whether to activate advanced features such as Global Money Transfer still assumes a level of sophistication that not all consumers have. For this reason, any new features that increase a consumer's fraud risk should default to not being available and should be introduced only with a comprehensive and ongoing consumer education program.

Giving consumers control of their digital account capabilities by allowing them to disable or adjust online features and limits can significantly reduce the risk of unauthorized transactions and fraud and will empower them to protect themselves by tailoring their account capabilities to their personal risk tolerance and usage patterns.

Such requirements may also stimulate competition and innovation among financial institutions to be able to offer enhanced validations as conveniently as possible.

Ensuring that banks offer these security options will lead to enhanced consumer trust and satisfaction as consumers are more likely to feel secure and confident in their banking relationship, knowing they have tools to protect their financial assets.

Requirement to detect fraud

QUESTION 3: SHOULD BANKS BE REQUIRED TO HAVE POLICIES AND PROCEDURES TO DETECT FRAUD AND SCAMS AND PREVENT CONSUMERS FROM BEING VICTIMIZED THAT MEET OR EXCEED A REGULATED STANDARD, AND, IF SO, WHAT POLICIES AND PROCEDURES WOULD BE MOST EFFECTIVE?

As noted above, 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 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 the patterns of fraudulent transactions outlined above in a more accurate and consistent manner and that this is an appropriate area for regulatory standards to be established.

Example 5 – Senior a repeated victim of fraud

Mr. H was a senior who held a chequing account and a credit card at his bank. He had previously been a victim of cryptocurrency fraud and had lost $26,000 in 2022. One day, he accessed his account, noticed his balance was low, and saw multiple unauthorized e-transfers totaling $13,800 from his chequing account to the same cryptocurrency recipient from the previous fraud.

He did not recognize the recipient and could not remember the how this fraud may have occurred. He reported the issue to his bank and the bank did not offer any compensation.

Liability limits

QUESTION 4: SHOULD A MAXIMUM LIABILITY THRESHOLD BE INTRODUCED FOR ACCOUNT HOLDERS WHO ARE VICTIMS OF UNAUTHORIZED TRANSACTIONS, REGARDLESS OF THE MEANS BY WHICH THEIR ACCOUNT FUNDS WERE ACCESSED (FOR EXAMPLE, CARD-BASED TRANSACTION, WIRE TRANSFER, OR ELECTRONIC FUNDS TRANSFER), AND UNDER WHAT CIRCUMSTANCES SHOULD CONSUMERS BE LIABLE FOR FUNDS LOST DUE TO UNAUTHORIZED TRANSACTIONS?

Canadians and Canadian banks are very familiar with consumer protection measures that limit their liability for fraudulent transactions. Currently, this protection is in place for credit card and debit card transactions but is not in place for other transactions. This discrepancy leads to confusion and dismay when consumers find that they have lost money from their bank account or credit line to a fraud or scam and are not protected.

Our experience has shown that many consumers' expectations of protection from fraud are not being met and we are concerned that this may be leading to an erosion of consumer confidence. This consumer expectation is likely based on the general understanding and advertising of "zero liability" protections for credit card products and the reputation of Canadian banks as safe, secure places for the safekeeping of consumer deposits.

For some consumers, this expectation of protection may also result from experience with the fraud prevention practices at banks which detect and prevent some suspicious transactions but miss others.

In addition, the wording used by banks to describe their own guarantees against fraud can be confusing in that they may promise fraud protection as long as the consumer "safeguards" their information. For many consumers, inadvertently clicking on a malicious link or being tricked by a fraudster is not a failure by them to safeguard.

We believe the liability limits and fraud detection and prevention practices currently applied to credit cards offer a good model for other banking products and services. Consumers have broad protections when using their credit cards which are provided under the Bank Act, provincial consumer protection acts, and card holder agreements. For example, the Bank Act section 627.33 provides that the consumer is not liable for an unauthorized transaction except if they acted with 'gross negligence' ('gross fault' in Quebec) to a maximum of $50. In these cases, the onus is on the bank to show gross negligence.

A standardized liability regime would be easier for consumers to understand and would establish a clear financial incentive for banks to invest in appropriate fraud detection, prevention and protection strategies.

While we support the introduction of a liability threshold comparable to that for credit cards, we also believe that it should be part of a broader, more comprehensive fraud prevention strategy for Canada that recognizes the important role that other stakeholders have to play in achieving this critical objective. Key stakeholders in fraud prevention include:

Example 6 – Fraud victim gives his card and PIN to the "police"

Mr. J was a new Canadian. He received a telephone call that appeared to be from his local police department. The caller identified themselves as a police officer and informed Mr. J that he had been the victim of a bank fraud and that his card had been compromised. The police officer said that he would need to impound Mr. J's bank card to use as evidence and told him that an officer would come to his home shortly to collect it. When the officer came to his door, Mr. J turned over his card and PIN.

Mr. J then called his bank to report the situation and his bank informed him that he had been the victim of a scam and deactivated his card. However, the fraudster had already withdrawn $2,500 from Mr. J's account.

- Law enforcement agencies tasked with enforcing the criminal laws
- Telecom and technology companies whose products and services are often involved in the commission of frauds
- Consumers who are ultimately responsible for protecting themselves, their devices and their information from criminals.

All of these stakeholders should be engaged in a comprehensive fraud prevention program for the protection of all Canadians.

The focus of this consultation, however, is on the fraud prevention potential of the banking sector, and as described above, in our view the sector could be doing more.

If a maximum liability threshold for consumers were implemented, it is likely this would provide a strong financial incentive for banks to ensure detection systems are optimally robust and comprehensive. For this reason, a liability regime could replace the separate regulatory obligations to detect and block fraudulent transactions discussed above. Instead of prescriptive legislation, a liability regime would establish outcomes-based financial incentives for institutions to develop and implement fraud detection and prevention mechanisms proactively.

Unauthorized transaction definition

QUESTION 5: WHAT CONSTITUTES AN UNAUTHORIZED TRANSACTION AND HOW SHOULD SUCH TRANSACTIONS BE DEFINED?

In fraud and scam cases, the distinction between authorized and unauthorized transactions can be blurry. It is clear that if a person's card or credentials are stolen from them, either physically or digitally, and they are not involved in the transaction in any way, the transaction is unauthorized. However, sometimes consumers will be involved in a transaction that is not what they believe it to be. For example, they may believe that they are sending money for a legitimate purpose only to find out later that they were dealing with a fraudster. In other situations, a consumer may enter their banking credentials or a one-time password believing that they are dealing with the police or their bank only to find out later that it was a criminal imposter. In these situations, while the consumer was personally involved in the transaction, they did not consent to the essential features of the transaction.

In our view, authorization should be defined as circumstances where a consumer correctly understands and consents to the key features of the transaction – i.e. the amount that they are transferring and to

Example 7 – Account credentials stolen

Ms. B had a chequing account with her bank that she often accessed through online banking. One day, Ms. B was having trouble logging into her online bank account and received a text message from what seemed to be her bank. She opened the message and clicked on the link provided, which took her to a website that looked like her bank's, and she entered her debit card number and password. Shortly after, she discovered that a bill payment of $24,300 had been sent from her account.

Ms. B complained that the bank should have prevented the bill payment and asked the bank for reimbursement. The bank did not agree to reimburse because she did not safeguard her banking information.

whom. The protection associated with unauthorized transactions could be subject to the consumer not being grossly negligent in their handling of their confidential information.

We believe that greater clarity on the definition of what constitutes authorization will provide greater clarity of accountability and increase fairness.

Data gathering requirements

QUESTION 6: SHOULD BANKS BE REQUIRED TO COLLECT AND REPORT ANONYMIZED, AGGREGATED DATA RELATED TO THE NATURE OF FRAUD AND SCAMS TARGETING THEIR CLIENTS, AND, IF SO, SHOULD BANKS BE REQUIRED TO REPORT THIS DATA TO FCAC?

We support establishing system-wide, aggregated data collection relating to frauds and scams as this would enhance fraud detection, pattern identification and the opportunity to create effective prevention strategies based on real experience.

We acknowledge the cost of gathering, aggregating, and analyzing such data will be significant. However, this investment would be justified if the insights from the gathered data are effectively used to make systemic improvements, enhance education and fraud prevention strategies, and increase consumer confidence.

In any such data aggregation system, FCAC must ensure that there is an appropriate mechanism for feedback of key data and insights back to the industry, the public, and any third-party service providers engaged in fraud prevention and detection.

Example 8 – Banking credentials used for unusual transaction

Mr. G held a home equity line of credit with his bank and often accessed his accounts through the bank's mobile application. He reviewed his accounts every month.

During one of his monthly reviews, he noticed an $85,000 bill payment had been sent from his home equity line of credit to a third party that he did not recognize. He had never made a bill payment from his home equity line of credit. He reported the unauthorized transaction to his bank and asked the bank to reimburse the amount of the bill payment. The bank did not agree to reimburse Mr. G because his banking information was used to make the bill payment.

Theme 5: Upholding world-class regulation

QUESTION 7: THE DEPARTMENT OF FINANCE IS SEEKING VIEWS ON PROVIDING REGULATORY PREDICTABILITY AND ON IMPROVING THE UNDERSTANDING OF REGULATORY ACTIONS AND IMPACTS. SUCH PROVISIONS COULD INCLUDE:

- COORDINATED PERIODIC ANNOUNCEMENTS ON LIKELY FORTHCOMING REGULATORY ACTIONS,
- CONDUCTING AND PUBLISHING IMPACT STATEMENTS OF REGULATORY ACTIONS,
- DEVELOPING A FORUM FOR COORDINATING AND COLLABORATING ON INTERNATIONAL ISSUES, AND
- SHARING OF INFORMATION ABOUT INTEGRITY AND SECURITY RISKS

We agree with all four proposed provisions. OBSI works at the intersection of federal, provincial, and territorial collaboration concerning financial services and consumer protection. In addition to resolving disputes for Canada's banking sector, OBSI also provides financial ombudservices for nearly all provincially regulated securities firms (including the investment subsidiaries of all Canadian banks), as well as many credit unions and their members.

We frequently consider both federal and provincial laws and regulations in our dispute resolution work, including provincal consumer protection legislation.

From our vantage point, it is clear that many historical distinctions between the "four pillars" of distinctly-regulated sectors, institutions and products are blurring or disappearing altogether. While banks, credit unions, investment firms and insurance firms offer distinct products and services, there is, increasingly, much overlap in their design, as well as in the types of challenges that firms and consumers experience in relation to them. This corresponds to an extensive and accelerating process of consolidation and integration within the financial industry.

Canadians are generally unaware of the jurisdictional regulatory structures that underly the regulation of the financial products and services they use on a daily basis. To the extent that coordination and harmonization between provincial jurisdictions and federal jurisdictions can be improved, consumers will benefit from greater consistency and predictability in the protections that are in place.

On the first point proposed in the Consultation Document, OBSI agrees that coordinated periodic announcements on likely forthcoming regulatory actions would be helpful and would support awareness and transparency for regulated entities and consumer organizations alike.

On the second point, we support the general premise that the likely impacts of any regulatory action should be considered before implementation. However, we would caution that for such impacts to be appropriately assesed, care must be taken to ensure that both regulated entities and consumer groups have been meaningfully consulted. We have observed that while regulated entities and industry organizations are generally well-placed to assess regulatory impacts on themselves and their stakeholders, consumer groups often lack the necessary resources to present their perspective as rigourously. Adding to this inequality of resources, the value of investor protection measures is often

more difficult to measure or quantify than the costs associated with implementation. As a possible solution to this imbalance, the federal government through FCAC could commission third-party experts to assess or directly evaluate the potential impacts of any proposed regulatory action on consumers, potentially in collaboration with provincial and territorial governments.

On the third point, we are very supportive of developing a forum for coordinating and collaborating on international issues. Many of the issues and challenges facing Canadian policymakers are shared by policymakers in other countries and coordination and collaboration can faciliate greater efficiency and better decision-making. Additionally, many policy issues facing the financial services sector are international in scope and would be best addressed through internationally coordinated responses. Challenges such as combatting fraud and other financial crime, effectively regulating fintechs in the consumer-driven banking field, and addressing the use of artificial intelligence in the financal services sector are all examples of fields that benefit from international coordination.

Regarding the fourth point, it is clear that Canadian consumer protection involves significant overlapping jurisdiction between the federal and various provincial and territorial regulators. In our experience, differences in the approaches taken by various provinces and the federal government on consumer protection issues can lead to confusion and gaps in protecton. We have observed that federally regulated entities operating across provinces sometimes have limited awareness of provincial consumer protection rules and this problem is compounded by the divergence of approaches to financial protection for consumers across different provinces. Greater harmonization in the consumer protection rules would benefit consumers and institutions alike, leading to improved protection and awareness for both consumers and entities operating across jurisdictions. We would observe that substantial harmonization already exists in the securities sector, where National Instruments used by provincial securities regulators benefit both consumers and securities entities operating nationwide. A similar approach to financial consumer protection in the credit union and banking sectors should be considered.

****

In closing, we thank you for giving us 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