Fintechs Canada

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

September 27, 2024

On behalf of Fintechs Canada, I would like to thank you for the opportunity to provide the Department of Finance with our perspective on the government's proposals to strengthen Canada's financial sector.

Fintechs Canada serves as the collective voice for the most innovative financial technology companies. Serving millions of Canadians from coast-to-coast, our membership consists of market-leading Canadian fintechs, fintech-friendly financial institutions, the technology companies that power the credit union space, and global fintech companies, among others. Our mission is to assist Canadians in accessing a more competitive and inclusive financial sector, while also protecting its integrity, stability and security.

In the rest of this submission, we provide our perspective in response to several of the government's proposals to strengthen Canada's financial sector.

Supporting competition and innovation

The best ways to promote financial sector competition

To build a more dynamic and competitive financial ecosystem, we recommend that the government prioritize the following:

1. **Establishing competition mandates for financial sector regulators.** Regulators such as the Office of the Superintendent of Financial Institutions, the Financial Consumer Agency of Canada, and the Bank of

Canada should be explicitly mandated to promote competition. This would ensure that they administer policy in a way that reduces barriers to entry and encourages diversity among financial service providers.

2. **Expanding access to and promoting fair pricing of critical payments infrastructure.** Payments infrastructure, such as the RTR, should be accessible to all market participants under fair and transparent pricing terms. Equal access to these networks is crucial for fostering competition and innovation, especially for smaller financial institutions.

3. **Modernizing Canada's approach to granting bank licenses.** Canada's bank licensing framework should be modernized to make it easier for non-traditional financial institutions to enter the market. By streamlining the licensing process and creating specific categories of licenses for digital-first and payment-focused institutions, the government can create a more diverse marketplace.

4. **Giving Canadians the right to control their financial data.** Implementing Canada's consumer-driven banking framework will give Canadians the right to securely control and share their financial data with third-party providers. This would empower consumers to switch between financial institutions more easily and increase competition by enabling new entrants to offer personalized, innovative services.

5. **Continuing the government's digitalization of money review.** Novel technologies, such as blockchain technology, and ecosystems, such as stablecoin arrangements, can introduce more competition in financial services, such as payments. But they also pose new risks that need to be managed before they're trusted and put to use. Since the launch of the government's digitalization of money review, there's been little communication about findings and the direction of any future work.

Merger and acquisition control not enough

While acquisition and merger control may prevent future conduct that may have anti-competitive effects, it does nothing to level the unlevel playing field today. New and small players entering the market often face structural barriers, including high capital requirements and complex regulatory frameworks enforced by OSFI, which demand extensive financial and operational readiness. Additionally, compliance with consumer protection, privacy, and cybersecurity regulations increases the burden on smaller players, making it difficult for them to compete with longstanding and established financial institutions.

Strengthen the ministerial application process for banking licences

While Canadians are most familiar with large, diversified financial institutions, the financial services landscape is evolving, with a growing number of nontraditional providers offering innovative services. Large diversified institutions serve the needs of some Canadians, but many have complex or specific financial requirements that exclude some consumers. New entrants, with different business models, can challenge the status quo and drive competition, which benefits consumers by creating more choice and encouraging better services.

We recommend that the ministerial application process should be strengthened by explicitly considering the public interest in allowing the entry of innovative financial institutions that don't necessarily conform to the expectations we have of what a traditional financial institution looks like. The Minister of Finance should be empowered to impose tailored terms and conditions that address the unique risks posed by these nontraditional institutions. This approach would enable new players to enter the market safely, while ensuring they adhere to high standards of compliance, risk management, and consumer protection.

Combating fraud

We know Canada has a fraud problem, but we don't know the extent of it. A recent Payments Canada survey found that almost 3 million Canadians were the victims of payments fraud in the first half of 2024. According to a ACI Worldwide report on real-time payments and fraud, Canada's fraud incidence rate is the eighth highest in the world.[1]

Unfortunately, this problem is expected to get worse. With the growing digitization of payments and the increased sophistication of cybercrime techniques, global losses due to payment fraud is expected to continue to rise, reaching $40.62 billion by 2027—a 25 percent increase from 2020.

We recommend the Department of Finance introduce:

---

[1] Identity theft and credit card fraud are on the decline, whereas confidence tricks are on the rise. Confidence tricks are when victims of fraud play are deceived into being part of the scheme. For example, they can be duped into sending a fraudster the money the fraudster is trying to steal. The money is often transferred using a real-time payment system so that the fraudster can withdraw or move the funds out of reach by the time the victim has discovered what's happened.

1. A general obligation for banks to fully reimburse their account holders in the event of any unauthorized movement of money, regardless of the payment instrument that was used.
2. A general obligation for banks to have policies and procedures in place to detect and prevent payments fraud.
3. An obligation for all federally regulated banks to collect and report anonymized and aggregated data about the number of fraudulent transactions by payment instrument, the average value of such transactions by payment instrument, and what percentage of these transactions were unauthorized by the account holder.

Obligation to reimburse should be general in law, but more specific elsewhere

We recommend only establishing a general obligation because legislation and regulation is not the ideal place to specify the circumstances under which a bank should reimburse an account holder in the event of unauthorized movement of money.

Prescribing in legislation or regulation what constitutes the unauthorized movement of money would be impractical, unless it was done differently for each payment instrument. There are different ways to authenticate an account holder and authorize them to move money, and they can vary from payment instrument to payment instrument. For example, the way mobile debit card transactions are authenticated and authorized differs from how cheque are: mobile debit transactions typically use real-time verification, including methods like biometric authentication or PIN codes, whereas cheques sometimes involve manual processes such as signature matching or account number validation.

Being specific in legislation and regulation about what is the unauthorized movement of money would also limit the ability of the industry to innovate. The way we pay is always changing, and so are the ways banks authenticate account holders and authorize transactions. But legislation and regulation are rarely amended quickly, and often amended long after the materialization of the facts and circumstances that necessitate an amendment in the first place.

Moreover, a general obligation may be sufficient to incentivize banks to work with each other and their partners to solve the problem. For example, banks could work with the different payment system operators to specify the circumstances under which customers must be fully reimbursed in the event of an unauthorized transaction in payment system rules. Banks and payment system operators could also work together to develop an industry-created, industry-governed, and industry-enforced code of conduct to address

payments fraud. This code can include criteria for when a transaction is considered unauthorized for each of the different payment instruments.[2]

If this approach does not produce desired results, the government could consider using its powers to compel payment system operators to develop and enforce criteria for when transactions related to their respective payment instruments are unauthorized.[3]

Obligation for policies and procedures should be general in law, but more specific elsewhere

We recommend only establishing a general obligation for banks to have policies and procedures to detect and prevent fraud because legislation and regulation is not the ideal place to specify the policies and procedures a bank must have to detect and prevent fraud.

The fraud-related risks of each payment differ by the instrument. For example, cheques are vulnerable to forgery and alteration, whereas mobile payments are susceptible to phishing attacks and other digital breaches. For cheques, a bank's policies and procedures may be geared toward detecting and preventing forgery and alteration of cheques, whereas, for mobile payments, a bank may rely on confirmation of payee, multi-factor authentication, encryption, and biometric verification to detect and prevent fraud.

A general obligation may incentivize banks to work with each other, as well as with different payment system operators, to agree on what should be a common set of policies and procedures to detect and prevent fraud. For example, due to the incidence of fraudsters using real-time payment systems to perpetrate phishing scams, operators of real-time account-to-account payment systems should offer participants centralized services to aid in detecting and preventing fraud. There may be some cases where banks should be required to use confirmation of payee to help account holders who may be falling victim to a phishing scam. Payment system operators may also choose to require their participants to have their own policies and procedures.

---

[2] The content of this code of conduct can be incorporated by reference in the rules of the different payment system operators. This could make the voluntary code not so voluntary after all. Like the debit and credit card code of conduct, this code of conduct for all payments to address fraud would become legally binding.

[3] This may be the Bank of Canada, which has power under the Payments Clearing and Settlement Act today. But it may also be the Minister of Finance, who has the power to designate payment systems and issue directives under the second part of the Canadian Payments Act.

If this does not work, the government could consider using its powers to compel payment system operators to work with banks and other participants to specify policies and procedures for detecting and preventing fraud.[4]

Require banks to collect and report anonymized and aggregated data

Banks should be required to collect and report data on confirmed fraud cases as we do not know the extent of Canada's fraud problem. The Canadian Anti-Fraud Centre (CAFC) says, as of June 30, Canadians have lost almost $300 million to fraudsters this year. But the CAFC cautions that fraud is grossly underreported in Canada, suggesting the problem is a lot bigger than we think.

Banks are in the best position to collect data related to the risk and cost of fraud to Canadians: they provide and monitor the accounts fraudsters are trying to access. They know when a fraudster gets access to an account, whether that's because they caught the fraudster in the act or because the account holder complained to the bank after the fact and the bank's investigation concluded a fraudster is to blame. Banks also know the amount of money that was stolen and what payment instrument was used to get the money out.

We recommend that the government regularly collect and report fraud data from banks to the CAFC. The CAFC should use this data to enhance its public reporting on fraud statistics.

Similar measures have been implemented in the UK, as payment service providers and banks are required to collect and submit data on the volume and value of fraudulent transactions to the Financial Conduct Authority. This data helps regulators identify trends, allocate resources effectively, and develop strategies to better predict, detect, and prevent fraudulent threats.

***

On behalf of Fintechs Canada, I would like to thank you again for the opportunity to provide the Department of Finance with our perspective on strengthening Canada's financial sector. We would gladly answer any questions you have about our proposals and discuss them in greater detail. We look forward to

[4] See footnote 3.

continuing to work with you and your team in an open, collaborative, and thoughtful way, as the Department of Finance is known to do by our sector.

Sincerely,

Alex Vronces
Executive Director, Fintechs Canada
1 Richmond Street West, Suite 200
Toronto, Ontario M5H 3W4