Fintechs Canada

Bank of Canada
234 Wellington St. W
Ottawa, ON K1A 0G9

May 21, 2024

On behalf of Fintechs Canada and its members, I would like to thank you for the opportunity to share our perspectives on the Bank of Canada's supervisory policies and guidelines on the following subjects:

- End-user funds safeguarding
- Operational risk and incident response
- Incident notifications
- Notice of significant change or new activity

Fintechs Canada is the unified voice for the most innovative financial technology companies in Canada. Serving millions of Canadians daily from across Canada, 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 support Canadians in accessing a more competitive and inclusive financial sector, while also upholding the sector's integrity, stability and security.

The Bank of Canada estimates there are more than a thousand payment service providers ("PSPs") in Canada, but we are concerned about the future of the industry. As we explain below, there are requirements for PSPs that are beyond their control or ability to meet.

It's critical that Canada's retail payments supervisory regime strike an appropriate balance between promoting a competitive and inclusive financial sector, while also upholding the sector's integrity, stability and security. Canada's financial sector is concentrated and shows signs of not being competitive enough.[1] If Canada's retail payments supervisory regime makes it unnecessarily difficult for PSPs to operate and expand in the Canadian market, the Bank of Canada will further suppress competition in Canada's financial sector.

In the rest of this submission, we identify those requirements that are challenging to implement and those that require clarification. For some, we recommend changes to the requirements to either make them easier to implement or clarify them.

1. End-user funds safeguarding

Requires clarification: what constitutes pre-funding?

- A PSP is not considered to be holding funds when it pre-funds a transaction or reserves funds to mitigate credit risk.
- PSPs hold funds for a variety of reasons, such as to mitigate chargeback or fraud-related risks in merchant transactions. PSPs are also required to pre-fund certain settlement accounts to allow their end-users to use retail payment services. In the latter case, funds are only used to pre-fund end-user transactions and prevent the funds from being used for any other purpose.
- The industry seeks clarification and recommends:
    a. That mitigating chargeback or fraud-related risk be included in the Bank of Canada's definition of what it means to reserve funds to mitigate credit risk.
    b. That the Bank of Canada consider allowing some end-user funds to be held in trust in a settlement account for the sole purpose of executing the end-users retail payment activities, so long as end-users are guaranteed to receive the funds in the event of a PSP's insolvency.[2]

---

[1] In its review of RBC's acquisition of HSBC, the Competition Bureau found that the financial sector is "concentrated, that there are by high barriers to entry and expansion in many of the relevant markets, and that conditions in certain of the relevant markets may facilitate coordinated behaviour among competitors."

[2] These are trust accounts where both end-users, as well as financial institutions and card networks, are beneficiaries. In practice, these accounts must only allow for the settlement of payment between end-users (i.e., segregated from PSPs' funds). The rights of financial institutions and payment networks' must not not trump the rights of end-users to their funds. Amounts must only be withdrawn from the trust account by the network provider or financial institution only after the end-user has initiated a payment. Agreements associated with the account between PSPs and financial institutions and payment networks must not allow for the settling any fees owed between

Requires clarification: set-off rights in cases where PSP is mitigating against certain risks

- A PSP must ensure its account provider has no right of set-off or compensation "in respect of the funds held in that account."
- In certain cases, PSPs may be owed funds by their customer in certain situations, such as chargebacks.
- The industry would benefit from clarification as to whether it may assert a right of set-off or compensation in the aforementioned cases.

Requires clarification: insurance for end-user funds safeguarding

- PSPs are required to hold funds in trust or in a bank account with a letter of guarantee or insurance.
- In some cases, PSPs will want or be required to obtain insurance. However, it's not clear whether such a market for insurance will emerge in Canada. Early conversations suggest there's not enough specificity in how the Bank of Canada describes the insurance to determine whether insurance can be offered at all.
- The industry would benefit from knowing more about the type of insurance products that will satisfy the Bank of Canada that a PSP is sufficiently safeguarding its end-user funds

Requires clarification: can PSPs safeguard all end-user funds?

- PSPs are required to safeguard any end-user funds in respect of a retail payment activity.
- In some cases, PSPs may hold end-user funds that are not in respect of a retail payment activity as defined by the Retail Payment Activities Act.
- The industry would benefit from clarification that PSPs may also safeguard end-user funds in respect of non-retail payment activities in the same account in which they safeguard funds in respect of retail payment activities.

---

the PSP, the financial institution, and the payment network. What's more, any funds remaining in such accounts post settlement of payments between end-users must be held in trust for the sole benefit of end users.

Challenging to implement: obtaining services from financial institutions

- We find the Bank of Canada's guidance helpful, but are worried that the requirements may be challenging to meet for reasons beyond the control of a payment service provider ("PSP").
- While the Bank of Canada's guidance clarifies that the range of entities that can offer PSPs trust or other acceptable accounts with guarantees ("end-user funds safeguarding services") is broad, it's not clear that any such entities will be in a position to offer such services when the time comes.
- Conversations with financial institutions suggest there are, in some cases, perceived barriers to offering PSPs end-user funds safeguarding services.
- To our knowledge, no insurance company is intending to provide insurance to support PSPs who can't obtain end-user funds safeguarding services from financial institutions.

Challenging to implement: segregating an end-user's funds in respect of a retail payment activity from an end-user's funds for other purposes

- The Bank of Canada requires that a PSP segregate end-user funds from any other funds, "including those that the PSP handles clients as part of business functions that are not related to a retail payment activity."
- Some PSPs aren't just PSPs and offer a range of financial services to their end-users, which are tied to the end-user's account also used for payment services.
- Some PSPs would find it operationally challenging to maintain separate accounts for the different types of financial services they offer a particular end-user. Some of these PSPs may prefer to safeguard all of their end-user's funds, regardless of whether the funds are held in respect of a retail payment activity or some other.
- We recommend the Bank of Canada clarify and allow PSPs to safeguard all of an end-user's funds in a single account.

Challenging to implement: customer-facing trust account documentation

- The Bank of Canada requires that, to "hold end-user funds in trust, a PSP must establish a trust arrangement with its end users that forms a valid express trust established under Canadian law."
- One interpretation of this requirement is that end users need to be party to the trust documentation a PSP has with the institution that offers the trust.
- This may require some PSPs who choose to safeguard end-user funds using multiple options simultaneously—for example, some funds in trust, and the rest in another account with a letter of guarantee and/or insurance—to enter into multiple agreements with end-users.
- To consider whether PSPs have satisfied the Bank of Canada's requirements for certainty of trust, certainty of objects, and certainty of intent, the Bank of Canada should consider all of the agreements a PSP has—not only the agreement a PSP has with its end-user.

2. Operational risk and incident response

Requires clarification: third-party risk management

- PSPs must identify and manage risks related to their use of third-party service providers. Management of such risks must involve everything from understanding the materiality of using third-party service providers to assessing and monitoring engaged third-party service providers, which can include creating compensating controls, such as termination plans.
- The industry would benefit from the following clarifications:
    a. Do these requirements apply to third-party service provider contracts that entered into prior to September 8, 2025?
    b. What is the standard of due diligence expected of a PSP when they are assessing and monitoring a third-party service provider? For example, are there materiality thresholds above which ongoing third-party audit attestations are appropriate, and below which less frequent self-attestation is appropriate?
    c. The definition of "third party" includes "affiliated entities" as a distinct category. But the definition of "third-party service provider" does not

expressly identify affiliates, while certain portions of the guidance seem to indicate that affiliates are considered third-party service providers. Are affiliates considered both third parties and third-party service providers?

Requires clarification: approvals and reporting

- The senior officer responsible for operational risk and incident response and the board (if any) of a PSP must approve a PSP's objectives, reliability targets and indicators.
- For large PSPs, the full inventory of objectives, reliability targets and indicators may be massive—for example, there may be hundreds, if not thousands, of reliability targets and indicators.
- The industry would benefit from knowing whether the Bank of Canada expects the senior officer and the board of a PSP to review and approve each and every of the PSP's objectives, reliability targets and indicators.

Requires clarification: ubiquity and interconnectedness

- The Bank of Canada will consider a range of factors to establish a PSP's ubiquity and interconnectedness.
- The industry would benefit from knowing whether the Bank of Canada has specific thresholds for each of the factors they will consider to establish a PSP's ubiquity and interconnectedness.

Requires clarification: reliability targets and indicators

- PSPs must establish measurable reliability targets for the performance of their retail payment activities and for the availability of their systems, data and information.
- The industry would benefit from knowing whether the Bank of Canada, in its supervision, will prescribe certain targets and indicators for all PSPs or whether the Bank of Canada will allow for variation of such targets and indicators across PSPs.

Requires clarification: detection and continuous monitoring

- A PSP must have a framework that describes the systems, policies, procedures, processes, controls in place to ensure continuous monitoring to promptly detect incidents, anomalous events that could indicate emerging operational risks and lapses in the implementation of the framework.
- "Promptly" means that the detection must be done quickly, while taking specific circumstances into account. In other words, unless PSPs have reasonable justification for delaying, they must prioritize the detection.
- The industry would benefit from knowing what the Bank of Canada may consider reasonable justification for delaying detection.

Challenging to implement: retroactive third-party risk management

- PSPs must identify and manage risks related to their use of third-party service providers. Management of such risks must involve everything from understanding the materiality of using third-party service providers to assessing and monitoring engaged third-party service providers, which can include creating compensating controls, such as termination plans.
- Retroactive application of these requirements will be challenging to implement in a timely manner, as complex third-party service relationships are carefully negotiated over long periods of time, and third-party service relationships can't be immediately terminated without significant disruptions to end-user services.

Challenging to implement: third-party risk management with large and inflexible firms

- PSPs must identify and manage risks related to their use of third-party service providers. Management of such risks must involve everything from understanding the materiality of using third-party service providers to assessing and monitoring engaged third-party service providers, which can include creating compensating controls, such as termination plans.
- In some cases, due to an imbalance of market power, PSPs may not be in a position to dictate terms and conditions with certain third-party service

providers in a timely manner. In such a case, a PSP may be required to do something by the Bank of Canada that is beyond the control of the PSP.

Challenging to implement: approvals and reporting

- The senior officer responsible for operational risk and incident response and the board (if any) of a PSP must approve a PSP's objectives, reliability targets and indicators.
- For large PSPs, the full inventory of objectives, reliability targets and indicators may be massive—for example, there may be hundreds, if not thousands, of reliability targets and indicators. In such cases, being required to report on and have approved each and every one may be infeasible.
- We recommend the Bank of Canada allow for some discretion in which reliability targets and indicators PSPs report, letting PSPs determine which are the most material to the risks posed by their payment activities.

3. Incident notifications

Requires clarification: incidents with a material impact

- The Bank of Canada's guidance describes incidents with a material impact. The guidance says such an event is one in which "any amount of an end user's funds held by a PSP has become lost or unavailable before the end user withdraws those funds or transfers them to another individual or entity." Examples include incidents in which "end-user funds held in that account are not accessible by end users in part or in full."
- There are incidents where end-user funds may be temporarily unavailable, but are nonetheless considered immaterial by industry. For example, consider a scenario where a tiny fraction of a percent of end-users may be temporarily unable to access their funds because of a service disruption, but service is restored soon thereafter and funds are still settled and made available to end-users within a PSP's transfer cut-off time.
- The industry would benefit from better understanding whether the Bank of Canada expects PSPs to report each and every such incident, regardless of its materiality, or whether the Bank of Canada will work with PSPs to establish more specific materiality thresholds.

Requires clarification: outages or slowdowns of retail payment activities

- The Bank of Canada requires notification if the "PSP experiences an outage of or slowdown in its retail payment activities for eight or more hours."
- In other jurisdictions, such as the EU, incident reports are triggered if materiality thresholds are surpassed. The materiality of an incident is determined not only by if an outage or a slowdown of a certain time materializes, but also if such happens in respect of a certain monetary volume of transactions or a certain percentage of customers affected.
- What's more, the guidance treats outages and slowdowns as if they are the same in materiality when they are not. An outrage is a full degradation of retail payment activities, whereas a slowdown is a minor to partial degradation, with some or many of the services to end-users still available.
- We recommend that the Bank of Canada align its guidance with international best practices, including allowing for the use of the aforementioned materiality thresholds. The Bank of Canada should work with PSPs to set such materiality thresholds in a way that is appropriate for the PSPs' specific facts and circumstances.

Requires clarification: reporting breaches of data

- According to the Bank of Canada's guidance, PSPs are required to notify the Bank of Canada no later than 24 hours after a breach of information has occurred and that breach of information results in or creates a risk of significant harm to an end user.
- Federal privacy legislation in Canada requires that companies report such breaches "as soon as feasible after you have determined that a breach of security safeguards involving a real risk of significant harm has occurred," which, in some cases, may not be consistent with the Bank of Canada's guidance.
- The industry would benefit from knowing whether the Bank of Canada's guidance is intended to be different from the requirement to report breaches in federal privacy legislation.
- We recommend that the government mirror the requirement to report breaches in federal privacy legislation to avoid imposing the costs of unnecessary regulatory complexity and disharmonization on PSPs.

Requires clarification: reporting integrity incidents

- The Bank of Canada's guidance says PSPs are required to report any incidents relating to the integrity of their retail payment activities. One of the examples includes "transaction processing errors (for example, payer sends $5 but payee receives $3).
- There are cases where such errors may be so exceptional in the operation of retail payment activities that they would not qualify as an incident affecting the integrity of a PSP's retail payment activities.
- The industry would benefit from knowing whether the Bank of Canada will work with PSPs to set materiality thresholds appropriate to the facts and circumstances.

4. Notice of significant change or new activity

Requires clarification: what is a material change?

- A PSP is expected to notify the Bank of Canada in the event there are any changes that may have a material impact on a retail payment activity.
- It's not clear from the guidance what may constitute a material impact. For example, in the event a PSP is changing from whom it receives cloud services, is it embarking on a significant change that may have a material impact on a retail payment activity?
- The industry would benefit from clarification as to what constitutes a change that may have a material impact on a retail payment activity.

***

On behalf of Fintechs Canada, I would like to thank you again for the opportunity to provide the Bank of Canada with our perspective on the aforementioned supervisory policies and guidelines. We look forward to meeting with you to discuss our feedback, as well as to continue to work with you and your team in an open, collaborative, and thoughtful way, as the Bank of Canada is known to do by our sector.

Sincerely,

Alex Vronces
Executive Director
1 Richmond Street West, Suite 300
Toronto, Ontario M5H 3W4