Fintechs Canada

Department of Finance
90 Elgin Street
Ottawa, Ontario K1A 0G5

March 28, 2023

On behalf of Fintechs Canada and its members, I would like to thank you for the opportunity to share our perspectives on the draft *Retail Payment Activities Act* regulations.

Fintechs Canada is a not-for-profit association that serves as the unified voice for fintechs in Canada. Our membership collectively serves millions of Canadians on a daily basis, and includes Canadian fintech market leaders, global fintech companies, payment networks, financial institutions, and start-ups and scale-ups that are defining the future of financial services in Canada and around the world.

Our mission is to improve the economic well-being of Canadians by making Canada's financial sector more competitive and innovative, as well as more stable and secure. A retail payments supervisory regime that adheres to the guiding principles of necessity, proportionality, consistency, and effectiveness is an important piece of the puzzle.

This is in line with the government's own objectives. In the 2021 budget, the federal government committed to making progress on a retail payments oversight framework "that would promote growth, innovation, and competition in digital payment services while making these payments services safer and more secure for consumers and businesses."

We applaud the Department of Finance for carrying out this important work. We support the intent of the *Retail Payment Activities Act* (the "RPAA") and the draft regulations (the "regulations"). The rest of this letter focuses on what needs to be improved.

But the regulations, as they're currently written, put the government's commitment at risk of being undeliverable. As they're currently written, the regulations violate the federal government's guiding principles:

- Necessity — supervision should address risks that lead to significant harm to end users and avoid duplication of existing rules;
- Proportionality — level of supervision should be commensurate with the level of risk posed by the payment activity;
- Consistency — similar risks should be subject to a similar level of supervision; and
- Effectiveness — requirements should be clear, accessible and easy to integrate within different payment services.

Failing to observe the guiding principles of necessity, proportionality, consistency, and effectiveness will have the unintended consequence of hindering growth, innovation and competition in retail payments, without making Canada's payments ecosystem any safer or more secure.For that reason, we believe the draft regulations need to be amended in order for the retail payments supervisory regime to deliver on the government's objectives.

1. Onerous and Prescriptive Requirements

The Issue(s)

We believe that many sections of the regulations violate the guiding principles of proportionality, necessity, and consistency.

Table 1. Status-quo wording in the regulations

Section	Draft Language
5(3)(a)	" If a payment service provider receives services from a third-party service provider, the risk management and incident response framework must address the means by which the payment service provider will — no less than once a year in respect of each of its third-party service providers and before entering into, renewing, extending or substantially amending a contract with a third-party service provider for the provision of a service related to a payment function — assess…"

8(1)(a)	"A payment service provider must carry out a review of its risk management and incident response framework at least once a year"
10(1)	"A payment service provider that has an internal or external auditor must ensure that, at least once every three years, a sufficiently skilled individual who has had no role in the establishment, implementation or maintenance of the payment service provider's risk management and incident response framework carries out an independent review of…"
15(6)(a)	"The payment service provider must review the safeguarding-of-funds framework to identify any gaps or vulnerabilities and determine what changes are required to ensure that the objectives set out in subsection (1) are met at least once a year…"
15(6)(b)	"The payment service provider must review the safeguarding-of-funds framework to identify any gaps or vulnerabilities and determine what changes are required to ensure that the objectives set out in subsection (1) are met following any change in the entities that provide the accounts in which end-user funds are held, the opening or closure of any such account or any change to the terms of the account agreement…"
16(1)	"At least once a year, a payment service provider referred to in subsection 20(1) of the Act must determine whether, at all times during the preceding year, the end-user funds held by it — or equivalent proceeds from any insurance or guarantee referred to in paragraph 20(1)(c) of the Act — would have been payable to end users in the case of an event referred to in subsection 14(3) of these Regulations."
17(1)	"A payment service provider referred to in subsection 20(1) of the Act must ensure that, at least once every two years, a sufficiently skilled individual who has had no role in the establishment, implementation or maintenance of the safeguarding-of-funds framework or in the making of the determination referred to subsection 16(1) carries out an independent review of the payment service provider's compliance with subsection 20(1) of the Act and sections 13 to 16 of these Regulations."

We agree with the intent of these requirements, but we don't believe it's necessary, proportional, or consistent to subject each and every payment service provider to the same requirements to deliver on the government's intention.

The Canadian payments ecosystem is heterogeneous, including in the degree to which payment service providers are ubiquitous and interconnected. By extension, the degree to which they pose risks to Canadians and the financial system varies. Therefore, the application of the aforementioned requirements should not be the same for each and every type of payment service provider.

On many occasions, the government has said the retail payments supervisory regime would be risk-based. But if the application of the RPAA and regulations were truly risk-based, a payment service provider with a few employees and whose only customers are friends and family would not have the same self- and third-party review triggers as a payment service provider that is the backbone of Canadian commerce and with thousands of employees. Moreover, payment service providers would not have to review their funds safeguarding framework any time there are *any* changes made to the terms and conditions of their account agreements, including immaterial ones. Each and every payment service provider would also not need to regularly review their relationships with every third-party service provider they have—they'd only need to do so in the context of third-party service providers that are critical to the retail payment activities they perform.

According to estimates from the federal government, there could be 2,500 payment service providers in Canada that will be subject to this regime. If these requirements remain unchanged, we believe that number is likely to be an overestimate.

Given what we know of what it costs to operate a payment service provider in Canada today, it's not unreasonable to infer that the compliance and assessment costs for a small payment service provider may be prohibitive. If the government does not make the application of the RPAA and regulations more proportional, necessary, and consistent, the government should expect a non-trivial number of payment service providers to consolidate or drop out of the market.

Our Feedback

The Department of Finance should make these requirements more necessary, proportional, and consistent by removing the more prescriptive and onerous elements from the regulations and letting the Bank of Canada include them in supervisory guidance.

Table 2. Our proposed wording in the regulations

Section	Current draft wording	Proposed wording
5(3)(a)	" If a payment service provider receives services from a third-party service provider, the risk management and incident response framework must address the means by which the payment service provider will — no less than once a year in respect of each of its third-party service providers and before entering into, renewing, extending or substantially amending a contract with a third-party service provider for the provision of a service related to a payment function — assess…"	" If a payment service provider receives services from a third-party service provider critical to the retail payment activities the payment service provider performs, the risk management and incident response framework must address the means by which the payment service provider will — before entering into, renewing, extending or substantially amending a contract with a third-party service provider for the provision of a service related to a payment function — assess…"
8(1)(a)	"A payment service provider must carry out a review of its risk management and incident response framework at least once a year"	*Removed (a)*
10(1)	"A payment service provider that has an internal or external auditor must ensure that, at least once every three years, a sufficiently skilled individual who has had no role in the establishment, implementation or maintenance of the payment service provider's risk management and incident response framework carries out an independent review of…"	"A payment service provider that has an internal or external auditor must ensure that a sufficiently skilled individual who has had no role in the establishment, implementation or maintenance of the payment service provider's risk management and incident response framework periodically carries out an independent review of…"
15(6)(a)	"The payment service provider must review the safeguarding-of-funds framework to identify any gaps or	*Removed (a)*

	vulnerabilities and determine what changes are required to ensure that the objectives set out in subsection (1) are met at least once a year…"	
15(6)(b)	"The payment service provider must review the safeguarding-of-funds framework to identify any gaps or vulnerabilities and determine what changes are required to ensure that the objectives set out in subsection (1) are met following any change in the entities that provide the accounts in which end-user funds are held, the opening or closure of any such account or any change to the terms of the account agreement…"	"The payment service provider must review the safeguarding-of-funds framework to identify any gaps or vulnerabilities and determine what changes are required to ensure that the objectives set out in subsection (1) are met following any change in the entities that provide the accounts in which end-user funds are held, the opening or closure of any such account or any material change to the terms of the account agreement…"
16(1)	"At least once a year, a payment service provider referred to in subsection 20(1) of the Act must determine whether, at all times during the preceding year, the end-user funds held by it — or equivalent proceeds from any insurance or guarantee referred to in paragraph 20(1)(c) of the Act — would have been payable to end users in the case of an event referred to in subsection 14(3) of these Regulations."	"From time to time, a payment service provider referred to in subsection 20(1) of the Act must determine whether, at all times during the preceding years, the end-user funds held by it — or equivalent proceeds from any insurance or guarantee referred to in paragraph 20(1)(c) of the Act — would have been payable to end users in the case of an event referred to in subsection 14(3) of these Regulations."
17(1)	"A payment service provider referred to in subsection 20(1) of the Act must ensure that, at least once every two years, a sufficiently skilled individual who has had no role in the	"A payment service provider referred to in subsection 20(1) of the Act must ensure that, from time to time, a sufficiently skilled individual who has had no role in the establishment,

	establishment, implementation or maintenance of the safeguarding-of-funds framework or in the making of the determination referred to subsection 16(1) carries out an independent review of the payment service provider's compliance with subsection 20(1) of the Act and sections 13 to 16 of these Regulations."	implementation or maintenance of the safeguarding-of-funds framework or in the making of the determination referred to subsection 16(1) carries out an independent review of the payment service provider's compliance with subsection 20(1) of the Act and sections 13 to 16 of these Regulations."

Our proposed changes are two-fold:

1. The first set of changes to the draft wording relax how frequently payment service providers must either review their frameworks themselves or engage a third-party to do the review for them. Our proposal also requires clarifying the frequency of reviews in supervisory guidance in a tiered manner, whereby the required frequency of reviews is more proportional to the risks posed by the payment service provider. In other words, not all payment service providers should have the same review triggers.
2. The second change is to add materiality and criticality thresholds to the requirements. The materiality threshold is added to the requirement to review the funds safeguarding framework in the event of a change to the account agreement, while the criticality threshold is added to the requirement to assess relationships with third-party service providers. The materiality and criticality thresholds should be clarified in supervisory guidance.

By removing the more onerous and prescriptive requirements from the regulations and putting them into guidance, it would also make the Bank of Canada a more nimble, responsive and effective regulator. Under our proposal, the Bank of Canada will have more flexibility to make changes to supervisory guidance as it sees fit. We believe the Bank of Canada should have the leeway to make the more prescriptive requirements more strict or more lenient, depending on what it learns in its new role as regulator of payment service providers, without requiring changes to the RPAA and regulations, which take more time to implement.

2. Lack of Clarity

The Issue(s)

We've found it challenging to comment on parts of the regulations because they're worded in a way that makes the implications of the wording difficult to understand.

Table 3. Ambiguous sections of the regulations

Section	Draft Language
3	"A retail payment activity that is performed as a service or business activity that is incidental to another service or business activity is, unless that other service or business activity consists of the performance of a payment function, a prescribed retail payment activity for the purpose of paragraph 6(d) of the Act."
8(1)(b)	"A payment service provider must carry out a review of its risk management and incident response framework before making any significant change to its operations or its policies, procedures, processes, controls or other means of managing operational risk…"
9(d)	"A payment service provider must establish and implement a testing methodology, for the purpose of identifying gaps in the effectiveness of, and vulnerabilities in, the systems, policies, procedures, processes, controls and other means provided for in its risk management and incident response framework, that provides for testing before the adoption of any significant change to the systems, policies, procedures, processes, controls or other means — or to any of the payment service provider's operations that will affect them — for the purpose of evaluating the effects of the change."
20(1)(a)	"The notice referred to in subsection 22(1) of the Act must be given to the Bank at least five business days before the day on which the payment service provider makes a significant change in the way it performs a retail payment activity or the day on which it performs a new retail payment activity."
6	"The risk management and incident response framework must have been approved by the senior officer referred to in subparagraph (1)(d)(ii) and the payment service provider's board of directors, if any,

	within the previous year and when each material change was made to the framework."
11(2)(b)	"The notice that must be given to the Bank under section 18 of the Act must be submitted using the electronic system provided by the Bank for that purpose…The notice must contain a description of the incident and its material impact on the individuals or entities referred to in paragraphs 18(1)(a) to (c) of the Act…"
12(1)(a)	"The notice that must be given under section 18 of the Act to an individual or entity referred to in any of paragraphs 18(1)(a) to (c) of the Act must be provided to each materially affected individual or entity using the most recent contact information provided by them to the payment service provider…"
12(2)(b)	"…The notice must include a description of the incident, including when it began, and the nature of its material impacts on the individuals or entities…"
23(8)	"For the purpose of paragraph 29(1)(k) of the Act, the prescribed information consists of, in respect of each third-party service provider that has or will have a material impact on the applicant's operational risks or the manner in which the applicant safeguards or plans to safeguard end-user funds…"
13–15	*Lacking clarification of how end-user funds may be safeguarded*

We agree with these requirements in principle, and so our only concern is that it's difficult to assess whether these requirements violate the government's guiding principles in practice:

- For example, depending on how the Bank of Canada clarifies the meaning of such words as "incidental," "significant," or "material," these requirements may or may not violate the guiding principles of effectiveness, necessity, consistency, and proportionality.
- The regulations don't specify the range of acceptable ways a payment service provider can safeguard end-user funds.
- Whether the scope of application will extend to Canadians who are using payment services in other countries is also unclear, as there is no mention at all of this in the regulations.

Without a better understanding of the Bank of Canada's thinking on what these words will mean, how end-user funds should be safeguarded, and what the scope of application is, it's not possible for us to comment on these requirements in an informed way at this time.

Our Feedback

The Department of Finance and the Bank of Canada should share draft supervisory guidance with the stakeholders before the regulations are finalized so that we can better assess the implications of the regulations and share more informed feedback.

We also recommend the government clarify in the regulations that:

- **Payment service providers will be able to safeguard funds as high-quality, liquid assets, such as government bonds or AAA-rated money market mutual funds.** We believe this should be permissible under Section 20(1)(b) of the RPAA.
- **Payment service providers whose customers are Canadians not located in Canada should be exempt from the scope of application of the RPAA.** Any extraterritorial application of the RPAA and regulations would be challenging for payment service providers who provide services in and must comply with the legal frameworks of multiple jurisdictions.

In the event it isn't appropriate to make these clarifications in the regulations, the Bank of Canada should make these clarifications in supervisory guidance.

***

Once again, I would like to thank you for the opportunity to share our thoughts on the regulations. Fintechs Canada is pleased to see the Department of Finance carry out this important work, and so we hope that you will take our perspective into consideration as you work to finalize the regulations.

Amending the regulations is critical to the federal government's 2021 commitment to "promote growth, innovation, and competition in digital payment services while making these payments services safer and more secure for consumers and businesses." Absent such changes, we fear a non-trivial number of payment service

providers will drop out of the market because of requirements that aren't proportional to the risks they pose.

In the meantime, Fintechs Canada would be more than happy to meet in order to discuss the current proposals, share our membership's experiences and insights, or answer any questions that you may have. We look forward to continuing the dialogue and creating a better, stronger retail payment supervision framework.

Sincerely,

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