

March 28, 2023

Nicolas Marion
Senior Director, Payments Policy
Department of Finance Canada
90 Elgin Street
Ottawa, Ontario K1A 0G5

VIA E-MAIL: fin.payments-paiements.fin@fin.gc.ca

The Canadian Prepaid Providers Organization (“[CPPO](#)”) is pleased to have the opportunity to submit comments on the Department of Finance’s proposed Regulations to enact the *Retail Payments Activities Act* (RPAA) published in Canada Gazette Part 1 on February 11, 2023.

The CPPO is a not-for-profit organization and the collective voice of the open-loop prepaid payments industry in Canada. The association is supported by major financial institutions, card networks, program managers and fintech innovators. The CPPO is focused on awareness and education to help consumers, governments and businesses understand the value of prepaid platforms and to enhance the experience associated with these solutions.

Open loop prepaid payments products serve as a catalyst for financial services innovation and represent one of the biggest growth segments in the industry. The Canadian open loop prepaid card market continues to grow at a rapid pace with total loads on all Canadian open loop prepaid card accounts amounting to about CA\$8.5 billion in 2021, up 76 per cent since 2019. This growth is expected to continue and to exceed CA\$17 billion in annual loads by 2025.¹ It is being driven by many new innovative financial products such as real-time wage access and familiar technologies like e-commerce delivery applications, both of which are being directly fueled by open loop prepaid products.

The RPAA and Canada’s Prepaid Ecosystem

While the CPPO is supportive of the RPAA as a mechanism to safeguard Canada’s financial system, we join other industry players who have identified several issues with the proposed Regulations, including the prescriptive nature and rapid implementation timeline.

Given the structure of Canada’s prepaid ecosystem and the unique participants involved, the CPPO’s submission focuses on concerns with the proposed Regulations that directly impact prepaid products and programs. Specifically, we would like to highlight concerns with the proposed Regulations as it relates to prepaid program managers.

Program managers are entities responsible for establishing and maintaining relationships with the participants involved in the payments value chain, including issuers, processors, sponsoring banks, payment networks, and card manufacturers. In addition, program managers handle the design, distribution, fulfillment, and marketing of prepaid payment programs.

The role of program managers is indicative of the complexity of Canada’s broader prepaid ecosystem. Further clarification and consideration on the scope and administration of the proposed Regulations are required to ensure the cost associated with running a prepaid program is not unduly increased which could hinder prepaid innovation in Canada.

¹ The Canadian Open-Loop Prepaid Card Market: 2021 Results and Forecast Update, Aite-Noverica Group. April 2022.

Definition of Payment Service Provider

Exemptions for Incidental Activity

The proposed Regulations exclude retail payment activities performed as a service or business activity that is incidental to another service or business activity that is not a payment function. We ask the Department to provide more details on what is considered “incidental”. In some PSP business models, end users retain nearly real-time access to any funds sent or received through the PSP, regardless of how system transactions or funds settlement occurs in the background. Since one of the primary goals of the RPAA is to manage operational risks and to safeguard end users, we request the Department to provide additional details on the definition of PSPs and consider additional exclusions where the end user has no risk of loss based on the contractual and operational design of a service.

Service Providers to Federally Regulated Financial Institutions

The draft Regulations do not apply to Federally Regulated Financial Institutions (FRFIs) because there is already sufficient oversight of those entities through other laws and regulatory bodies. We ask the Department to also consider exempting entities that act as service providers to FRFIs. FRFIs are responsible for performing due diligence on their suppliers and monitoring them to ensure that they meet adequate service levels and provide for sufficient operational resilience. As the RPAA obligations are significant, it would add a material burden to companies that act in this service provider capacity, without adding clear additional benefits.

Risk Management and Incident Response

Risk Management Framework and Testing

The draft Regulations require a PSP to establish and implement a customized testing methodology to identifying design and operating effectiveness gaps in its Risk Management Framework controls. Although not directly regulated today, many PSPs provide third-party services to regulated entities such as banks or other financial institutions or are subject to payment network rules. Most of these entities are contractually required to comply with existing data security standards (such as Payment Card Industry Data Security Standards or SOC 2 Type 2 reports covering Security, Availability, Processing Integrity, Confidentiality, and Privacy). We encourage the Department to provide PSPs the flexibility to leverage existing Risk Management Framework and testing standards to achieve the necessity principles articulated in the Impact Statement.

Third Party Service Providers

The draft Regulations require a PSP to include third-party service providers in its Risk Management Framework. We propose that the Department provide PSPs with the flexibility to develop materiality and criticality thresholds to determine which third-party service providers should be included in the Risk Management Framework. The draft Regulations are quite prescriptive in the oversight requirements but do not clearly provide this flexibility, and implementing the requirements across all contractual service provider relationships would create an unintentionally high level of administrative burden that does not lead to a material benefit.

Reporting

Incident Reporting

It is not clear from the wording of either the RPAA or the draft Regulations which incidents are considered “material”, or how these obligations are meant to interact with existing legislative obligations and

regulatory standards. Many PSPs are already subject to federal and provincial privacy laws that have similar reporting requirements. Additionally, Federally Regulated Financial Institutions must comply with the Office of the Superintendent of Financial Institutions (OSFI) regulatory incident reporting regime, which requires initial reporting within 24 hours (or sooner, if possible). The OSFI Technology and Cyber Security Incident Reporting guidance set out criteria for when a technology or cyber security incident will trigger reporting requirements.

To eliminate any duplication of RPAA obligations and existing rules, we ask the Department to consider these existing reporting regimes to allow organizations to appropriately tailor their compliance efforts. For example, PSPs acting as service providers to federally regulated financial institutions, or those that are already subject to provincial privacy regulations, should be exempted from the RPAA incident reporting provisions. Confusion as to the interoperability of the RPAA and privacy legislative regimes could lead to potentially unnecessary administrative and compliance costs.

Significant Change or New Activity Notification Obligations

The annual report discussed in the draft Regulations is very comprehensive and detailed, including everything from Risk Management Framework changes and operational risks identified to hundreds of different data points relating to the PSP's ubiquity and interconnectedness. The prescriptiveness of these data points is very burdensome and it is unclear how this data would provide material benefit to the Department in its oversight obligations, absent a robust AI solution. We therefore call for a more proportionate reporting requirement that would provide the Bank of Canada with the necessary level of detail to undertake its oversight function.

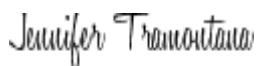
Compliance Costs

As described above, program managers act as third-party service providers. Given third-party service providers interact directly with FRFIs or payment networks, they are already subject to existing data security standards. Many third-party service providers are also required to meet federal and provincial reporting requirements. The costs associated with the additional requirements and fees under the proposed Regulations would disproportionately impact third-party service providers which already meet various obligations under existing regulatory regimes. Moreover, the level of risk associated with third-party service providers who interact with regulated entities (and the related obligations) is arguably less compared to entities that are not captured by any existing regulatory framework. Accordingly, we encourage Finance Canada to exempt third-party service providers to FRFIs and payment networks from the regime.

Conclusion

The CPPO thanks you for the opportunity to submit these comments. If you have any questions or require any additional information, please do not hesitate to contact us.

Yours sincerely,



Jennifer Tramontana
Executive Director, CPPO