ELECTRONIC TRANSACTIONS ASSOCIATION
1620 L Street NW, Suite 1020
Washington, DC 20036
202.828.2635
electran.org

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 Electronic Transactions Association (**ETA**) submits these comments in response to the Department of Finance's publication of the draft regulations to enact the *Retail Payments Activities Act* (RPAA) published in Canada Gazette Part 1 on February 11, 2023. We hope that these comments assist the government in understanding the key considerations of the payments industry with respect to the implementation of the RPAA.

ETA is the leading trade association for the payments industry, representing over 500 companies that offer electronic transaction processing products and services. ETA's members include financial institutions, mobile payment service providers, mobile wallet providers and non-bank online lenders that make commercial loans, primarily to small businesses, either directly or in partnership with other lenders. ETA member companies are creating innovative offerings in financial services, revolutionizing the way commerce is conducted with safe, convenient, and rewarding payment solutions and lending alternatives.

ETA remains supportive of the RPAA as it seeks to safeguard the integrity of the Canadian financial system while protecting Canadian consumers. The implementation of the RPAA will also allow Canada to keep pace with global financial regulatory advancements, joining countries and regions such as the United Kingdom (UK) and the European Union (EU) with a modernized payment service framework.

However, ETA and its members are concerned by several issues, in particular the overly prescriptive nature of the RPAA which is not in line with established global standards or the principles articulated in the Impact Statement of necessity, proportionality, consistency, and effectiveness. We believe there is a need for further regulatory clarity on matters such as the scope and changes with respect to the safeguarding of funds. If these issues are not addressed, we are of the view that this will hamper new entrants into the market, stifle innovation and affect Canada's status as a business and financial hub.

An Overly Prescriptive Approach

ETA supports a principles-based approach to the regulation of payment service providers (PSP) and is concerned with the overly prescriptive nature of the RPAA. For example, the RPAA proposes that all registered PSPs include information on the PSP's ubiquity and interconnectedness, some examples of which are: the value of end-user funds held; the volume of electronic fund transfers in relation to which they performed a retail payment activity; and the number of end users. On the other hand, no such requirement exists for the UK and EU regulatory regimes. Instead, their reporting requirements have chosen to focus specifically on fraud and assessment of security risks.

We urge you to take a principles-based approach that aligns with the guiding principles established at the outset of this process, namely: necessity, proportionality, consistency, and effectiveness. Ultimately, such onerous requirements as those proposed are likely to result in additional regulatory friction due to the RPAA not being harmonized with other leading jurisdictions as the E.U. and the U.K. We therefore strongly request that this global alignment continue to be viewed as a guiding principle in the development of the final regulations and guidance documents.

Some of these concerns are addressed in greater detail in the comments below.

Geographic Scope

ETA submits that establishing clear parameters for what kind of entities or payment activities will be regulated are key requirements for a successful regulatory framework. While we appreciate that the draft regulations note that the Bank of Canada (Bank) will develop guidance that provides further direction to PSPs regarding the Act's scope, this issue is foundational to the entire regime and should be clarified with a sense of urgency.

A key issue pertains to the operationalization of a geographical scope, a matter of importance for many PSPs given their global footprint. While the RPAA has set out a framework outlining the conditions in which the location of a PSP and an end user determine whether a payment activity is regulated, we find that there is a lack of clarity in certain situations. Given that the scope of the regime is a foundational issue impacting key pillars of the regime – risk management and incident response, funds safeguarding, information for annual report – it is imperative that PSPs receive clarity on this in a timely manner so they can prepare for the regime to come into force.

As an example of the problem, consider a Canadian individual currently working overseas in Thailand that uses a PSP that has a Canadian presence to send money to his/her parents in the UK. Assume that the Canadian individual in Thailand would use their Canadian identity document for the transaction. In these circumstances, the proposed geographic scope of the RPAA would require the Thailand-based PSP to comply with Canadian law in respect of the transaction. Under this use case, a PSP will be required to reprogram their systems globally to trigger a flag whenever "a Canadian" or a person with Canadian identification or a Canadian payment card engages in a transaction. Any such system modifications require significant resources and capital investment. Moreover, depending on the business model of the PSP, it may require the cooperation and coordination of both agents and other service providers in numerous countries, some of which the PSP may not be able to directly control.

As another example, digital wallets have become a popular means of payment, especially for people in the Indo Pacific region. These digital wallets typically provide stored value or "e-money" accounts to their individual users, where the user can top up their digital wallet from a funding source such as their bank account and use the balance in their digital wallet to make payment at a merchant in-store or online. Increasingly, providers of digital wallets are partnering with PSPs to enable cross-border acceptance of their digital wallets. A foreign licensed PSP providing digital wallet services to users in an Indo Pacific country may partner with a Canadian licensed PSP, which provides merchant acquiring services to Canadian merchants. This partnership would enable the Canadian merchants serviced by the Canadian PSP to accept payment from the Indo Pacific consumers using those consumers' preferred digital wallet as a payment method, whether online or in-store when the Indo-Pacific consumer is travelling in Canada. In such a scenario, we would expect that the foreign PSP providing the

ELECTRONIC TRANSACTIONS ASSOCIATION
1620 L Street NW, Suite 1020
Washington, DC 20036
202.828.2635
electran.org

digital wallet services to foreign users would not be subject to the Act because it is not performing any retail payment activity for end users in Canada. To our knowledge, this would be generally consistent with the regulatory framework in other countries such as the UK and in the EU.

The operational burdens of implementing these changes not only affects efficiency but also diverts resources away from PSPs that could otherwise be allocated to other commercial activities, fraud prevention, and anti-money laundering initiatives. The ETA and its members do not believe that the compliance costs and related burden for complying with the RPAA globally for those end users that have a Canadian "connection" contributes meaningfully to public confidence in Canadian retail payment systems, one of the objectives of the RPAA. Furthermore, we do not believe that Canadians would expect the protections of the RPAA to extend to them when they are engaging in a transaction outside of the country where there is no "leg in" or "leg out "of Canada as part of the transaction.

In addition to the foregoing, as a result of the inefficiencies that would be created by the extra-territorial application of RPAA, consumers will see more friction in their payments experience. From the perspective of a PSP, instead of reprogramming its systems globally to recognize transactions with a Canadian connection, it would be more efficient and cost effective for it to instead disallow Canadians from engaging in transactions outside of Canada. Although this will assist PSPs in dealing with their increased compliance burdens, it will lead to a negative customer experience for Canadian end-users, in direct contradiction to the stated goals of the RPAA.

From a policy perspective, we understand there may be a desire to ensure geographic scope in this context is aligned with that of the Financial Transactions and Reports Analysis Centre of Canada ("FINTRAC"), the regulator which oversees the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (the "PCMLTFA"), Canada's anti-money laundering ("AML") regime. With the greatest of deference, the policy considerations that underlie the PCMLTFA and those which underlie a retail payments framework are completely different. While there may be policy considerations that support the extra-territorial application of the AML laws, the same considerations do not apply to retail payments, and such a consideration appears to be unprecedented across jurisdictions.

Specifically, the object of the PCMLTFA at its core is to detect and deter money laundering and the financing of terrorist activities. In that respect, as the Bank is likely aware, one of the stages of money laundering is "layering" which often involves moving money out of the country of origin to separate the illicit money from its source. As such, in the AML context, it is justifiable from a policy perspective, to require foreign money services businesses to report to FINTRAC the international movement of funds where a person with a connection to Canada is involved. Receiving these electronic funds transfer reports allows FINTRAC to "follow the money" as part of its role in detecting money laundering. However, in the context of retail payments, it is submitted that there is no similar policy principle that would require a PSP to comply with Canadian law when they carry on business in the normal course outside of Canada. As such, the ETA and its members strongly believe that aligning the approach of the RPAA to the one used in the AML context is misguided.

Consequently, ETA submits that there should not be an extraterritorial application (ie: the RPAA should not apply to Canadians transacting outside of Canada) under the RPAA. We urge inclusion of language clarifying geographic scope in the final regulations to implement the RPAA.

Safeguarding of Funds
ETA shares the government's goals of protecting consumers in the event of a PSP insolvency and appreciates that the RPAA legislation contemplates flexibility for PSPs to meet safeguarding obligations. Avoiding a one-size-fits-all approach will allow the RPAA to appropriately cover a wide range of business models in the payments industry while ensuring consumer protection is not compromised. We believe that as currently proposed, the RPAA is not representative of all PSPs' operations as they relate to holding of end-user funds and encourage further changes to reflect these operational realities.

First, how funds are safeguarded is a key area that needs to be addressed urgently. Section 20.1(c) of the Act pertaining to funds safeguarding appears to require that funds be held in a segregated account with insurance or a financial guarantee on top of that. The requirement for companies to obtain financial assurances through the provision of a letter of credit or through private insurance in addition to the need to segregate user funds would be the most stringent requirement we are aware of. It is also worth noting that the cost of securing a financial guarantee can be substantial and differ between providers. This could create an unintended competitive disadvantage, could translate to higher costs for consumers, and underscores the importance of allowing PSPs reasonable flexibility in this area.

ETA therefore submits that the RPAA should allow PSPs to safeguard user funds by either obtaining a letter of credit or appropriate private insurance or by segregating user funds. A standalone guarantee as a safeguarding option is the kind of common-sense flexibility ETA members have experienced in other jurisdictions including the EU Payment Services Directive (2015/2366) (PSD2) and in many U.S. jurisdictions as well. We would like to propose this approach for your consideration. Additionally, as consistent with other regulatory regimes, we ask that the final regulations allow for high quality bonds and other investment grade or higher instruments to qualify for safeguarding purposes at their market value. This can allow some products to be offered to consumers at low prices and drives market competitiveness.

Second, ETA feels that the need to review the safeguarding of funds framework whenever there is a "change to the terms of the account agreement" is not consistent with the proportionality goal of the legislation. Frequent changes to the terms of the account agreement are a norm in the financial industry, as fees are added/revised, new privacy protections or changes to other terms are introduced. However, these terms are not material to the safeguarding of funds, and for a PSP to review their entire funds safeguarding framework imposes an unnecessarily onerous burden. As such, we would recommend that the requirement for a review of the safeguarding framework only be triggered where the account agreement is amended in a material or significant way that relates to the PSP's obligation to safeguard funds.

Third, given the globalized nature of payment services, it is inevitable that funds may be held in different jurisdictions. Additionally, funds in transit or held for less than 24 hours are also key features of the PSP industry. Therefore, ETA submits that the draft regulations also require clarification around when the safeguarding obligation arises and when it ends. From a materiality perspective, considering the various PSP business models, we feel calculation of funds required to be safeguarded should exclude those funds paid out to beneficiaries by the end of the business day following the day of transaction initiation.

Fourth, ETA asserts the importance of having clear guidance for when obligations to safeguard end-user funds begin and end, particularly by starting with clarifying that the safeguarding

requirements do not apply where a PSP pre-funds, or extends credit, for transactions prior to receiving end user funds from the payor. The formal recognition of the existence of diverse business models along with the clarification that some PSPs do not hold end user funds, and therefore should not be captured by the funds safeguarding requirements would be helpful.

Finally, ETA notes that in the occurrence of an insolvency event, PSPs are to ensure that funds are paid to end users as soon as feasible. In such circumstances, PSPs have no control in respect of the distribution of funds, as this will be up to the receiver or administrator that takes control of the PSP's estate. In keeping with the foregoing, there should be some provision in the regulations to allow the proceeds of any guarantee or letter of credit to be payable to the Bank of Canada (or as it directs) upon the occurrence of an insolvency event. Otherwise, the proceeds of the letter of credit can be seen as an asset of the estate.

We note that if there is concern in respect of the treatment of end-user funds, these can be easily addressed by giving these assets priority under the *Companies' Creditors Arrangement Act* or the *Bankruptcy and Insolvency Act*. It is submitted that these matters are best dealt with in insolvency legislation as opposed to by imposing requirements on PSPs that have no legal control in the event of an insolvency.

Penalties and Violations

ETA recognizes the importance of compliance in the payments industry, and the draft regulations have been developed to maintain the integrity of the industry and protect consumers. However, any proposed measures to address non-compliance with the Act should also be "consistent" and "proportionate" – which have been identified as key principles guiding the draft regulations. As the draft regulations currently stand, they are inconsistent with existing administrative monetary penalties.

Specifically, ETA submits that the administrative monetary penalties (AMP) are excessive when compared to other similar statutes such as the PCMLTFA. This concern is further exacerbated by a lack of clarity on the designation of provisions. As an example, the penalty range for serious and very serious violations under the PCMLTFA are up to $100,000 and $500,000 respectively. On the other hand, the RPAA proposes up to $1,000,000 and $10,000,000 be imposed for serious and very serious violations respectively. In our view, the regulatory considerations given to retail payments far exceed those for money-laundering and terrorism financing and do not align well with the logic of proportionality, a point we have consistently highlighted in this submission.

We note that an administrative monetary penalty framework serves to discourage undesirable conduct in the payments industry. On the other hand, if a penalty framework is taken to the extreme and applied in the context of retail payments where the standard of significance is arguably lower than other statutes such as the PCMLTFA, it will position Canada as a heavy-handed place for PSPs. Additionally, it is equally important that guidance on the kinds of factors taken into consideration for the criteria of harm, history and degree of negligence/intention should be provided so PSPs can adopt the appropriate compliance measures as soon as possible.

Risk Management Framework

ETA appreciates the draft guidance discussing alignment with global practices with respect to operational risk management. Part of this alignment should be recognizing that PSPs can leverage their global risk framework or other currently existing frameworks to comply with the key concepts outlined in draft regulations. For example, there should be clarity around what

constitutes a "senior officer" with recognition that this individual may not necessarily be housed within the Canadian entity but nonetheless has the responsibility and expertise to oversee the PSPs compliance with the risk framework envisioned in the draft regulations.

Additionally, the bespoke compliance testing concept in the draft Regulations to identify gaps or vulnerabilities in the Framework does not align with existing data security standards many PSPs are already subject to. For example, a PSP acting as a service provider to a regulated financial institution will typically agree contractually to certain control standards such as SOC 2. While a prescribed methodology remains appropriate for entities not otherwise subject to existing standards, the Regulations should permit flexibility by allowing entities to leverage existing standards in designing their compliance testing approach. This will also align with retail payments regimes in other jurisdictions such as the European Union's Guidelines on ICT and security risk management, where they have refrained from adopting an overly prescriptive approach in favour of a more principle based one.

ETA also appreciates the need for requiring a PSP to identify all assets (including systems, data and information) and business processes that are associated with a PSPs performance of retail payment activities and to classify them according to their sensitivity and criticality. However, in this day and age of data breaches, we are concerned that the preparation and existence of such a document by PSPs as part of a risk management framework is a roadmap for any hacker that may be able to break into a PSP's systems. Similarly, details outlining every potential cause of a PSP's operational risks could also be exploited by nefarious actors. Hence, we find that the prescriptive nature of these documents in and of themselves are highly likely to give rise to operational risks.

Lastly, while the proposed Regulations recognize the diversity in the payments ecosystem by incorporating the principle of proportionality, there is also a challenge in applying this to a PSP's risk management framework. For example, a lack of insight into the entire Canadian payments market may prevent a PSP from accurately determining whether its framework is proportional to the impact that a reduction, deterioration, or breakdown of its retail payment activities could have on end users and other PSPs. We believe that this issue could also be addressed by ensuring that the framework is more aligned with global standards to allow PSPs to leverage their existing systems and controls.

Reporting Requirements

The payments industry is a rapidly changing space and ETA notes that the Act has been developed to manage the process of change. However, there are several areas where we would benefit from further guidance and clarity.

Firstly, we would like to receive more guidance and clarity on what kind of situations for a PSP fall under making "a significant change in the way it performs a retail payment activity" or "before they perform a new retail payment activity" when it comes to providing a significant change report. For example, will the notice be triggered when it comes to adding a new payment method in addition to what is being offered? Is a report required if the terms of service are changed? What if a new feature to an already existing service is added by a PSP? For example, Singapore's *Payment Services Act* has made it clear that any changes pertaining to operating rules or settlement procedures need to be reported and it is important that any reporting guidelines are specific enough to help PSPs meet their regulatory obligations.

For the above-mentioned scenarios, some of them relate to day-to-day operational matters and may not constitute a significant change in the PSP's business model. Therefore, we believe that more clarity is required here, and one possible solution could involve mandating a notice only where there is a resulting change to a PSP's operational risks.

ETA also believes that further harmonization is required between the various reporting requirements under the RPAA to make compliance more manageable for PSPs.

Pursuant to this, ETA recommends:

1. That further clarity around the purpose of this reporting be provided, particularly around how will this be used and/or assessed;
2. that the five-day prior notification period under the **significant change report provisions** be changed to one day to better reflect the operational realities of PSPs and their need for rapid change management processes; and
3. that the timelines for conducting **the biennial independent review** under the safeguarding of funds provisions be extended to every three years. This would be aligned with the three-year timeline established with the independent review process required under the risk management and incident response measures of the RPAA.

Third Party Service Providers

ETA appreciates the risk some third-party service providers ("TPSPs") may introduce into the retail payments system and supports efforts to appropriately mitigate this risk. However, given a single PSP may rely on dozens or hundreds of TPSPs, many of which do not provide services specific to payment activities covered by the Act, additional clarification is needed regarding the scope of TPSP coverage. ETA recommends inclusion of a materiality threshold to help PSPs understand which TPSPs will require detailed operational risk assessments. Given the requirement to assess a TPSP's data security infrastructure and risk management practices at least annually, without a materiality threshold PSPs may find themselves spending significant compliance resources performing assessments on TPSPs unwarranted by the proportional risk of that TPSP. The Regulations as they stand would require assessments of TPSPs without regard to their implication in payment activities. This means that facility management services, tablet providers or mail couriers could be captured by the requirement to report and cause someone to be unregistered under the Regulation. We don't believe this is the intention of the legislators or the regulator, therefore, to avoid confusion, a clarification and materiality threshold would be helpful.

Record Keeping

ETA has no major concerns with the record keeping requirement but feels that greater clarity could be provided on the matter. In respect of the record keeping requirements set out in section 40, the requirement is to maintain records "until the day that is 5 years after the day on which they cease to demonstrate the PSP's compliance with a current obligation." Should the Act be amended or the business of the PSP changes where "current obligations" cease to exist, we would like some guidance on what kind of record keeping requirements are applicable in such a situation.

ELECTRONIC TRANSACTIONS ASSOCIATION
1620 L Street NW, Suite 1020
Washington, DC 20036
202.828.2635
electran.org

Implementation Timeline

Considering the overall aim of these retail payments requirements, which are to ensure that Canadians can reliably use payment services and to promote the safety and integrity of the financial system and proper functioning of the economy, it is critical that PSPs be given sufficient lead time to effectively build out these robust requirements rather than operate under tight timelines. We note many PSPs have dedicated existing compliance resources to implement new MSB registration and reporting requirements established by FINTRAC in 2022, limiting in practice PSP's ability to dedicate compliance resources to RPAA implementation. Therefore, ETA submits that the regulations should be adopted on a fair and reasonable timeline. Given the complexity of the compliance obligations contained in the RPAA, ETA suggests that a 24-month implementation would be reasonable for PSPs to comply with the new regime after all aspects of the regime are finalized. However, any delay should not hinder efforts underway to expand membership in Payments Canada to prove the ability for PSPs to access the Real Time Rail.

Conclusion

ETA would be pleased to discuss the comments herein with Finance Canada and the Bank of Canada to ensure the perspective of the payments industry is well understood. ETA thanks you for the opportunity to submit these comments.

Yours respectfully,

Scott Talbott
Senior Vice President
Electronic Transactions Association