ASSOCIATION DES BANQUIERS CANADIENS
CANADIAN BANKERS ASSOCIATION

Box 348, Commerce Court West
199 Bay Street, 30th Floor
Toronto, Ontario, Canada M5L 1G2
www.cba.ca

Darren Hannah
Vice-President
Finance, Risk & Prudential Policy
Tel: (416) 362-6093 Ext. 236
dhannah@cba.ca

October 4, 2017

Financial Systems Division
Financial Sector Policy Branch
Department of Finance Canada
Email: fin.payments-paiements.fin@canada.ca

The CBA[1] is pleased to provide our responses and comments on the Department of Finance's consultation on the development of a New Retail Payments Oversight Framework. Banks are strong proponents of innovation and competition in the financial services sector, as innovation and competition in this area leads to better products and services and improved convenience for consumers and other end users. While the recent emergence of companies that focus exclusively on financial technology ("fintechs") has had a positive impact on the marketplace overall, we believe rapid advances in technology and business models by these fintechs when they act as payment service providers ("PSPs") have introduced risks that can impact end users of those payment services and the stability of the payments system. As a result, we welcome your efforts to regulate PSPs.

Banks in Canada have long been leaders in the development and adoption of new technologies and innovation that make banking and payments safe, simple and convenient for customers while also fostering customer trust and confidence. Banks invest heavily in technology to support payments and the banking system generally, with the six largest banks in Canada spending $76.5 billion on technology between 2006 and 2016, including $6.3 billion in 2016 alone.

We concur that the overarching objective of establishing a new oversight framework should be to ensure the retail payments ecosystem evolves in such a way that it remains reliable and safe for end users. We are pleased that the proposed framework recognizes the importance of principles-based requirements that balance the ability of PSPs to innovate while ensuring basic standards for

[1] The Canadian Bankers Association is the voice of more than 60 domestic and foreign banks that help drive Canada's economic growth and prosperity. The CBA advocates for public policies that contribute to a sound, thriving banking system to ensure Canadians can succeed in their financial goals. www.cba.ca.

end-user safety and the stability of the retail payments system. This approach is consistent with international trends.

We believe that the proposed risk-based oversight framework has the potential to increase confidence in the market and allow businesses to research, invest and innovate. As discussed below, there are a number of matters that require clarification and further analysis to deliver the goals of the oversight framework.

Key Comments / Recommendations

Supporting a Flexible, Principles-based Approach

The CBA supports the concept that an oversight framework should be guided by the principles of necessity, proportionality, consistency and effectiveness. Rules should be targeted to address the specific risks that exist, and should sufficiently address the degree of risk posed by a payment activity without posing undue burden on any provider.

Creating a balance between effective oversight and encouraging innovation also means that measures should strive to be principles-based. We are pleased that the Government's consultation paper highlights the importance of principles-based requirements to accommodate the diversity of business models in the retail payments sector. Given the speed with which retail payments is evolving, the framework will also need to be flexible and nimble to remain relevant and current with technology.

Imposing detailed and prescriptive rules such as the information that must be disclosed to end users, for example, seems inconsistent with the goal of a principles-based approach. If the Government deems it necessary to set rules that contain this level of detail, we recommend that such detail be set out in regulations to ensure they can be more easily modified and updated to keep pace with changes in the market.

Creating a Modern, Harmonized and Coordinated National Framework

It will be critically important for the Government's new regulatory framework to promote a unified and coordinated approach to payments across Canada. Given how interconnected payments systems are, and that payment risk extends across provincial boundaries, the oversight framework should be anchored under federal jurisdiction.

In addition, every effort should be made to harmonize the oversight framework with existing rules so that the framework is as comprehensive as possible for the functions of payments, while recognizing and avoiding duplication with other oversight frameworks. This includes taking into account the robust rules already applicable to banks (i.e., under the *Bank Act)* and rules and standards that other entities such as Payments Canada are responsible for so that there is no duplication or conflict.

While there may be a number of vehicles that could be considered to encourage coordination among various jurisdictions and regulatory bodies across Canada, we recommend that a federal/provincial cooperative forum or council on regulation be established to develop common standards that would be adopted by the various regulators. This type of structure would not only be helpful in ensuring that all payment providers in Canada are subject to a single and national set of rules, but would also be consistent with the Government's broader goal of providing advisory services to users of the system, as noted in the consultation paper. We believe that a single cooperative body that could speak with one voice on payments issues could be a particularly effective way to ensure that the Government's broader goals on safety, efficiency and user interests are achieved on a national basis in a consistent, cohesive, coordinated and comprehensive manner.

Given that technological advances and changing end-user expectations are a key driver of market change in the payments ecosystem, it is equally important that parallel changes are made to other statutes governing financial services (such as the *Bank Act* and the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act ("PCMLTFA")* to ensure a consistent regulatory framework. It is necessary for this legislation to be modified by, for example, allowing the use of new identity verification methods and enhancing the delivery of disclosures through electronic means. The scope of entity reporting sectors under the PCMLTFA will also need to be revisited, along with the interpretation by the Financial Transactions and Reports Analysis Centre of Canada of what qualifies as a money service business. Creating a modern set of rules, applicable to the activities of an entity, as opposed to an entity type, supports the ongoing evolution of payments in Canada and ensures that consumers and other end-user needs are served and protected.

Liability

The liability rules for unauthorized transactions and errors should be designed to mitigate and control risks created by the expanded number of participants. If the liability rules are not appropriately structured and clear to all participants, there may be the unintended consequence that the core of the payments system is de-stabilized by the periphery.

As we explain in more detail later in our response, we believe the framework should clarify that liability reside with those responsible for the risk and in the best position to manage it. For example, when a payment service provider performing the Payment Initiation function (as defined in the framework) is used to initiate a payment, it should be liable for any payment incidents within its sphere. The payer's bank and payee's bank should not be held liable for payment incidents that the PSP initiating the payment is responsible for. This is the approach taken in the framework governing retail payments in Europe, which we believe creates fairness and ensures the right incentives are in place for all participants in the payments chain to have the right security and authentication procedures in place.

We also believe that an important component of any liability framework is to ensure that clear disclosures are provided to end users regarding the allocation of responsibilities. This will assist end users in understanding who to contact when disputes arise regarding unauthorized transactions or transaction errors, and the process they should follow to seek recourse.

CBA's Responses to Specific Consultation Questions

Perimeter (Section 5.1)

1. Is the proposed perimeter appropriate to mitigate risks in retail payments?

We support the concept that the perimeter should extend to all payment instruments or functions regardless of the type of organization providing the payment activity. A functional approach to oversight of retail payments is the same model that other jurisdictions follow such as Australia's regulation of Non-cash Payment Facilities, which is considered to be any method for making a payment other than through the physical delivery of currency.[2]

Section 5.1 of the consultation paper notes that the framework is intended to cover a wide array of transactions conducted through various payment methods, "such as credit card transactions, online payments". From our perspective, following a functional oversight model means that the legislation should avoid referring to payment mode (e.g., card) or channel (e.g., online) when describing scope. To ensure legislative and regulatory flexibility and accommodate future innovation, it would be best to limit all references to payment modes and channels, where possible.

Consistent with adopting a risk-based oversight framework, we agree that certain types of transactions posing limited risk to end users should be excluded from oversight and that these exclusions should extend to transactions conducted by service providers such as banks that are already subject to substantially similar requirements under other statutes. However, greater clarity is required with respect to certain exclusions listed in the consultation paper. The second exclusion in the list for transactions conducted by agents should be limited to professionals that are specifically regulated with respect to their payment functions. As it relates to store cards and shopping mall cards, some are quite sophisticated and may include auto-reloadable features, may retain personally identifiable information (unlike gift cards), and some provide access to a large number of merchants. Funds can also be held in large sums for lengthy periods of time. Rather than excluding these types of cards outright, we recommend considering addressing the need for proportionality through tiering based on the attributes of that payment method, such as those noted above.

[2] See Australia Corporations Act 2001 and the ASIC Corporations (Non-cash Payment Facilities) Instrument 2016/211

We agree with the position taken in the consultation paper on virtual currencies. We recommend that care is taken to ensure standards are agnostic about the type of currency used so that updates to regulations are not required once virtual currencies become more frequent and involve large values.

To ensure that provisions of the oversight framework extend to all payment services provided in Canada, we recommend that language be incorporated confirming that oversight pertains to all PSPs that conduct payment functions in Canada or on behalf of Canadian businesses and/or end users, regardless of where the PSP is domiciled.

The perimeter should also distinguish business users from other end users so that rules are specific to the type of risks and protections required. Business users do not require the same degree of oversight and therefore principles related to disclosures, dispute resolution, and allocation of liability can be less rigid than the corresponding standards that are set for consumers.

End-User Fund Safeguarding (Section 5.2.1)

2. *Is the proposed requirement to place end-user funds in trust accounts combined with detailed record keeping, annual filings and the regulator's compliance tools (described in Annex C) appropriate?*

We agree with the idea that PSPs should deposit funds held on behalf of customers in trust accounts and segregated from other accounts. However, these requirements should apply at all times to end-user funds held by PSPs – i.e., not just when they are held for the duration of overnight or longer. There is no legal basis for allowing end-user funds to be co-mingled with a PSP's own assets at any time. To ensure end-user funds are kept safe and protected from a PSP's creditors, for example, they should at all times be maintained in segregated trust accounts that are distinguishable from the PSP's own operating accounts.

In addition to the trust account requirements, we also suggest that minimum capital requirements be applied that are scaled for size, which is the model used today in Europe. PSPs that hold funds on behalf of end users ought to meet similar requirements as federal deposit taking institutions do, including making PSPs subject to comparable AML regulations (i.e., suspicious transaction reporting thresholds); and setting out robust operational standards.

We also recommend that the balances held by PSPs be subject to something similar to unclaimed balances procedures on bank accounts where unclaimed funds are provided to the Government after an extended period without contact from the end user.

Regarding the Compliance Tools described in Annex C, there should be specific requirements added for PSPs to report any legal or regulatory actions commenced against the PSP in any jurisdiction where it operates, including investigations, claims, charges, penalties, etc. This is particularly important for PSPs located abroad, so that supervisory authorities in Canada are aware

of alleged misconduct and can use the information in any investigation or inquiry that is commenced in Canada.

3. *Should any exemptions from the trust account requirements exist (e.g., where funds held are below a specified per-user threshold (e.g., $100) or where funds are only held for a short period of time)? Would additional measures be desirable?*

We question the use of exemptions from the trust account requirements given that they erode the Government's underlying policy goal regarding the protection of end-user funds. Care should be taken to minimize the use of exemptions, and additional restrictions should be considered such as a prohibition on trust accounts being overdrawn by PSPs for any reason.

Operational Standards (Section 5.2.2)

4. *Are the proposed measures to address operational risks appropriate?*

Operational risk covers a broad spectrum and can therefore be complex. We recommend that each measure be reviewed against each of the five payment functions to determine whether each is required for all functions. We realize that all functions are required in the course of a payment and are inextricably linked, but a more detailed review would be beneficial to ensure that the measures are not overly burdensome vis-à-vis the risk of that function.

Dispute Resolution (Section 5.2.4)

5. *Are the proposed essential elements for a complaint handling process appropriate?*

We recognize the importance of ensuring that mechanisms are in place to assist end users in resolving disputes and seeking redress for issues that may arise when using payment services. We strongly support including dispute resolution measures in the oversight framework.

As mentioned in our key recommendations, we believe that clear disclosure of responsibilities regarding liability and complaint handling should be provided to end users. This will assist end users in understanding who to contact when disputes arise regarding unauthorized transactions or transaction errors, and the process they should follow to seek recourse.

The dispute resolution elements, and the proposed approach to using an external complaint body, focus on the end user so it would make sense that only the payment functions that have a direct PSP/end user business relationship be subject to these elements (much like the disclosure principles).

Liability (Section 5.2.5)

6. *Are the proposed measures regarding liability in case of errors and unauthorized transactions appropriate?*

Rules governing liability for unauthorized transactions are an essential component of the oversight framework and will strengthen protections for end users and other stakeholders in the payments ecosystem. We appreciate the fact that the proposed measures are largely consistent with the approach that's followed in existing liability rules related to payments when it comes to ensuring that end users will be liable where they fail to act responsibly or where they contributed to the unauthorized use.

The proposal contemplates that the payment-authorizing PSP would bear liability for unauthorized transactions or errors, and that liability could be shifted to intermediaries through agreements with those parties. It is not clear what the term "payment authorizing PSP" means. Section 5.1 refers to a PSP that is involved in "authorization and transmission", which "provides services to approve a transaction", but that may not be what is meant by a "payment authorizing PSP". Depending on how a payment transaction is structured, separate entities could (1) authenticate the identity of the payor providing instructions; (2) verify that the method of payment is valid; and (3) verify that there are sufficient funds in the payor's account. It is unclear in the proposed oversight framework which of the three functions above is expected to bear liability for unauthorized transactions.

In general, we support the premise that there should be accountability for resolving disputes and providing recourse to end users. Liability should be assigned to the entity that causes the loss and that is in the best position to manage it, particularly if there are no agreements directly between the PSPs involved in a payment transaction chain.

The framework governing payment services in the EU (the revised Payment Services Directive) takes the position that liability should be appropriately allocated between the payment service provider servicing the account and the payment initiation service provider involved in the transaction in order to compel them to take responsibility for the respective parts of the transaction that are under their control. Articles 72 and 73 stipulate that if the payment transaction is initiated through a payment initiation service provider, the payment initiation service provider is liable for unauthorized transactions unless it can prove that the payment transaction was authenticated, accurately recorded and not affected by a technical breakdown or other deficiency. In the absence of this proof, the payment initiation service provider is expected to compensate the institution holding the funds for restoring funds to the customer's account.[3]

Defining and determining liability in a payment transaction is an extremely complex issue given that there are potentially numerous parties involved, and a myriad of potential scenarios that can lead to

[3] Directive (EU) 2015/2366 on payment services, found at http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015L2366&from=EN

loss for end users. For example, consider a situation where a customer has accounts at multiple PSPs and uses the same credentials at both PSPs in order to login, access their account, and execute a payment. If a fraudster successfully hacks one of those accounts because of weak security and uses the credentials to breach the account at the second PSP, is the first PSP liable for both breaches? What, if any, liability does the end user have as a result of using the same credentials? This example highlights the need for the Government to carefully consider the liability provisions and various case studies so that liability is made clear and assigned appropriately for the benefit of end users and all participants, thereby promoting fairness in the payment system.

Registration (Section 5.2.6)

7. Is the level of information that would be required at registration appropriate?

The CBA supports the proposal that requires PSP registration so that a mechanism exists to identify and track PSPs in the sector and monitor their compliance with applicable regulation. This is consistent with the requirements in place in other jurisdictions such as Australia and the UK in their oversight of "Non-cash Payment Facilities" and "Payment Institutions", respectively.

We recommend ensuring that the framework captures all PSPs that conduct payment functions in Canada or on behalf of Canadian businesses and/or end users. Specific to Annex B, the information seems to be overlooking the need to capture the payment function(s) to be performed by a PSP. These should be identified at registration, since some information listed would only apply to certain functions (e.g., #15 would only apply to those holding funds).

Additionally, compliance information should be required as part of registration including whether there have been any legal or regulatory actions commenced against the PSP in any jurisdiction where it operates including investigations, claims, charges, penalties, etc. Regarding Annex B, item #3 should include confirmation of good standing/status; #8 should include a requirement for an organizational chart/business structure to be provided with ownership information. These measures would provide greater transparency regarding the PSP's structure and its fitness to operate in Canada.

8. Are the proposed criteria for registration adequate?

The CBA strongly supports the proposal requiring owners and directors to undergo a background check to determine whether there has previously been convictions of fraud and other financial offences. However, it is equally important to extend those checks to executives and employees, just as banks are required to do, to mitigate against risks associated with insider cyber attacks, identity theft and fraud.

In relation to cyber security, registrants should be required to develop and maintain appropriate cyber security policies since cyber contagion has the ability to spread throughout the ecosystem. The risk and impact of this threat is not proportional to the size or scale of an organization – the

interconnected nature of payments puts all players at risk in connection with a single incident. It is suggested that policies and procedures should be equivalent to those that banks adhere to under the Cyber Security Self-Assessment Guidance published by OSFI on October 28, 2013.

In addition, the CBA agrees that the framework should promote compliance with the PCMLTFA by allowing the registrar to deny or revoke a PSP's registration if the PSP is deemed to have violated anti-money laundering and terrorist financing laws.

Innovation and Competition (Section 5.3)

9. Stakeholders are invited to provide views on approaches for tiering of specific proposed measures.

The CBA supports the concept that the requirements and the level of oversight should be proportionate to the risks posed. One goal should be to strike a balance between alleviating unnecessary costs and burden for PSPs and minimizing risk and harm to end users. The specific thresholds or criteria to be considered in a tiered model might take into consideration the scale of activity, degree of risk to end users, and whether participants are subject to other regulatory oversight.

The other goal is to balance the opportunity of innovation/competition with the need to promote the safety and soundness of the economy and manage macro prudential risk. The Government must not lose focus of the importance of the retail payments system to Canada's financial markets and Canada's financial stability. Capital requirements, limits on the use of end-user funds, and compliance with the anti-money laundering laws are important measures to strengthen the solvency and viability of PSPs and ensure they remain prosperous in the long-term.

10. Would the framework sufficiently promote innovation and competition?

The proposed framework recognizes the importance of principles-based requirements, the tiering of measures, and the need to minimize overlap with other regulatory frameworks. In the CBA's view, these are key features of an approach that balances the freedom for PSPs to innovate and the need for basic standards to promote safety of end users and stability of the payments system. Standards play an important role in helping small firms grow and evolve because they enhance consumer confidence and trust, which is a necessary condition for businesses to prosper.

Conclusion

Canada's financial services sector is undergoing a significant transformation, which is being spurred by advances in technology and innovation in retail payments. Creating an effective oversight framework will ensure all participants abide by appropriate and consistent standards of conduct to ensure the safety and security of the payment systems, its users and their funds. This will lead to more robust and competitive payment systems, encourage innovation and build on the strengths of existing payment solutions and technologies.

We appreciate having the opportunity to contribute to this consultation process. Please feel free to contact me if you would like to discuss any of the topics contained in this letter.

Sincerely,