Open Banking

02/11/2019

Submission to Finance Canada

ASSOCIATION DES BANQUIERS CANADIENS
CANADIAN BANKERS ASSOCIATION

Introduction

The Canadian Bankers Association is pleased to provide this submission in response to Finance Canada's January 2019 consultation paper (the **Consultation Paper**) on the merits of open banking in Canada. The banking industry is a strong proponent of a competitive and innovative financial services sector that uses rapidly developing technological solutions to better serve customers and meet evolving client expectations. Canadian banks are leaders in the adoption of new technologies that make banking simple and convenient for customers while also fostering customer trust and confidence. Constantly looking to the future, banks have established internal innovation hubs and partnered with outside organizations, including universities, incubators, and technology companies, in an effort to pursue, design and deliver digital innovations and solutions for bank customers.

As key stakeholders that would be significantly impacted by developments relating to open banking in Canada, the banking industry welcomes the opportunity to continue to work with the federal government on fully understanding the benefits and risks of open banking. This submission sets out our views on the uniquely Canadian context around open banking and focuses on responding to questions raised in the Consultation Paper, in the following order:

- **Canadian Context**
- **Potential Risks of Open Banking**
    1. **Consumer Protection**
    2. **Privacy and Confidentiality**
    3. **Financial Crime**
    4. **Financial Stability**
- **Role of Federal Government**

We look forward to exploring other pertinent issues with the federal government as its review of the merits of open banking proceeds.

Canadian Context

We agree with the commentary in the Consultation Paper that open banking offers benefits to consumers, including small businesses, financial institutions such as banks, and other third party financial service providers (TPPs). Provided the inherent risks associated with open banking are effectively managed, open banking provides an opportunity for consumers to more easily share their financial transaction data and benefit from new and innovative products and services customized to their needs.

As the Consultation Paper observes, different jurisdictions have adopted varying approaches based on the level and scope of market activity, and the range of catalysts that triggered market and policy responses in those jurisdictions. Several jurisdictions started exploring open banking in the aftermath of the 2008-2009 financial crisis. Systemic failure of banking systems, and the subsequent loss of trust required the marketplace and policy makers to search out alternatives to the banking system. Canada is unlike these jurisdictions insofar as Canadian financial institutions survived the financial crisis with a high degree of public trust. As the government continues its examination of open banking models being explored, introduced or implemented in other jurisdictions, we strongly encourage the government to assess these models through the uniquely Canadian lens.

As the Consultation Paper notes, the broader context of policy initiatives affecting the financial services industry in Canada must be considered carefully at the same time as the merits of open banking are being reviewed. We agree with the Consultation Paper's specific highlighting of the payments modernization initiative, the national digital and data strategy consultations, and cyber security strategy. Regarding the payments modernization initiative in particular, we agree with the commentary in the Consultation Paper that, should the government proceed with an open banking approach that incorporates payments initiation, its appropriate staging and alignment with payments modernization will need further discussion. As Finance is aware, the scope and roadmap of the payments modernization initiative in Canada is particularly ambitious and involves significant complexity, costs and resources for stakeholders. Efforts should also be made to enhance customer choice by ensuring TPPs and other sources of customer information are required to exchange this information on similar terms, where the customer has requested such exchange. More broadly speaking, the government may wish to consider customer data in the context of industries other than banking, and how facilitating greater customer control over their own data in those industries could drive innovation. In the context of examining the interplay between open banking and these other initiatives, it is imperative that Finance Canada continue discussion and collaboration with the policy-makers and regulators that are directly involved in these related initiatives, as well as those regulators that are engaged on various issues relating to open banking such as the Office of the Privacy Commissioner (OPC) and the Office of the Superintendent of Financial Institutions.

To date, Canada's financial institutions have invested heavily on building the infrastructure necessary to protect the privacy and security of customer financial transaction data. Providing data access to an increasing number of TPPs will result in additional, incremental operational and technical requirements for infrastructure and new systems, which in turn will require ongoing maintenance, enhancement and

training. Consideration of open banking models should therefore include examination of how other market participants can contribute to the foundational capabilities that financial institutions have established, and continue to improve, in support and furtherance of appropriate data governance and protection.

Potential Risks of Open Banking

The potential benefits of open banking require the associated risks to be addressed and mitigated through appropriate allocation of responsibilities between all participants whether consumers, financial institutions, or other TPPs.

The following sets out our views regarding the potential risks and mitigation strategies associated with the four areas highlighted in the Consultation Paper.

1. Consumer Protection

We support the observations in the Consultation Paper relating to the importance of consumer protection. Customers' personal and confidential information ought to be secure and protected at all times by all open banking ecosystem participants, including TPPs. Customer information should only be shared with informed customer consent obtained in a transparent manner that allows the customer to understand how their financial transaction data will be used and secured. Customers should also be provided sufficient information to make informed decisions about the services a TPP offers, including any financial services or products that a TPP may suggest as value-add services. It is also crucial for customers to understand the mechanisms of recourse and redress available to them in the event of a data breach or misuse of financial transaction data by a TPP. Once TPPs receive financial transaction data, they become accountable for the information and therefore liable for mishandling it. In this respect, consideration should be given to what requirements TPPs must adhere to in order to fulfill their financial obligations to customers – e.g., capital, liquidity, insurance, etc. This is important particularly where the TPP is a technology business, and not subject to the same comprehensive regulatory oversight as Canadian banks. Canadian open banking development must also consider how various participants can be regulated, where there are regulatory gaps, including TPPs that are not federally-regulated financial institutions, non-domestic TPPs, and TPPs who may gain access downstream. It is important for customers to be protected regardless of the nature of the TPP involved and, as new business models emerge, that customers do not lose any protections that are afforded to them by regulations applicable to financial institutions.

Our discussion below about the privacy implications of open banking provides further commentary related to the specific consumer protection elements that are necessary to ensure that consumers truly benefit from open banking.

2. Privacy and Confidentiality

It is a priority for financial institutions to invest substantially in technology, infrastructure, and training to protect the personal and confidential information entrusted to them by their customers. However, this is a shared responsibility of all participants in open banking including customers and other TPPs. The handling of highly sensitive personal and confidential information is key to any open banking model, and necessitates informed customer consent and transparency, consistent standards for the responsible use and management of customer financial transaction data, and the safeguarding of that data.

A high level of trust will be required to support the success of open banking. A key component of fostering trust and widespread adoption is ensuring that the principle of confidentiality of data is considered and respected. The expectation of confidentiality is one of the foundations that lead to the trust that customers have in the traditional custodians of their financial transaction data. Another aspect is the responsible use and management of financial transaction data. Financial institutions have developed and adhere to standards to ensure there is no misuse of data, that data is protected. The *Personal Information Protection and Electronic Documents Act* (PIPEDA) is comprehensive, technology-neutral, and principle-based legislation that governs all Canadian organizations in combination with substantially similar provincial legislation where implemented. PIPEDA provides the framework and flexibility needed to address emerging privacy law concerns related to personal information exchanged for purposes of open banking.

Under PIPEDA, knowledge and consent are generally required for the collection, use, or disclosure of personal information. Consent is only valid where it is reasonable to expect that an individual would understand the nature, purpose, and consequences of the collection, use, or disclosure of personal information. And, the collection, use, and disclosure of personal information collected is restricted to the purposes that a reasonable person would consider appropriate in the circumstances. In accordance with these requirements, TPPs should clearly explain to customers what specific information they will be collecting, how they are going to use it, who they will be sharing it with, how a customer's rights may be limited, and any potential harms that may arise from customers' sharing their information. TPPs should also explain to customers what their recourse is in the event of a breach or compromise of their personal information and provide a simple process by which customers can revoke consent. Disclosure to customers is important to maintain customer control over their financial transaction data and must be

combined with the security and other requirements on TPPs and other ecosystem participants. In this respect, the OPC has broad oversight and enforcement power, including the ability to conduct audits of the privacy policies and practices of organizations, to enter into compliance agreements with organizations, and to refer non-compliance to the Federal Court.

The Accountability principle under Schedule 1 of PIPEDA is of particular importance in the context of open banking. This principle provides that an organization is responsible for personal information under its control. Where a customer directs a financial institution to disclose information about that customer to a TPP, the TPP is then solely responsible under PIPEDA for the customer's personal information under its control.[1] Given TPPs are accountable for the personal information in their possession in an open banking environment, it is crucial they are compliant with the requirements under PIPEDA – including appropriate safeguarding of data based on its sensitivity. Consideration must be given to the varying degrees of sophistication among participants in open banking, and the need to ensure all participants understand their rights and responsibilities under PIPEDA. This could be reinforced in different ways, including contractual arrangements among participants, industry standards, or an accreditation process for TPPs through an industry or regulatory body similar to the model suggested in the Retail Payments Oversight Framework[2]. In addition, the OPC's ongoing privacy education and awareness campaigns are essential requirements. Customers should understand the distinction between the consent they provide to their financial institution to share financial transaction data with a TPP, and the consent they give to the TPP which will govern the TPP's use of the financial transaction data and the customer's recourse to the TPP.

It is important to note that, although PIPEDA applies to personal information, the obligations of confidentiality by financial institutions extend beyond personal information and TPPs should be expected to meet similar requirements outlined above for the protection of confidential customer financial transaction data information more broadly. It is also essential to clearly delineate customer financial transactional data from proprietary information (e.g. enriched data) of financial institutions. Recognizing and preserving the ability of financial institutions to protect their proprietary information will be necessary in the open banking context.

Disclosure to customers is important to maintain customer control over their financial transaction data, however it is not sufficient for a robust system and must be supported by security and other requirements

[1] This disclosure, at the customer's direction, is distinguishable from when an organization outsources the processing of personal information to a third party. In that case, the transferring organization remains accountable as the information remains under its control – see OPC's interpretation bulletin on accountability https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_02_acc/

[2] Under the Retail Payments Oversight Framework, all payment service providers would be required to register with a "designated federal retail payments regulator" and provide the complete list of information required by the regulator.

on TPPs and other system participants. Open banking must include appropriate security and other safeguards for financial transaction data across the ecosystem and meaningful customer redress in order to achieve the benefits discussed in the Consultation Paper.

3. Financial Crime

There are specific characteristics of open banking which increase the risk of financial crime, including data proliferation, increased connectivity and the use of log-in credentials by TPPs to access data on behalf of customers. It is crucial to understand these risks, and how they can be managed by open banking participants.

When more parties transmit and store financial transaction data (i.e., data proliferation), the risks of account takeover and identify theft increase in many ways – particularly if security safeguards, including authentication standards, across market participants are subject to varying levels of controls. The increased connectivity of open banking increases the number of network vulnerabilities. The ability of financial institutions to use financial transaction data for multifactor authentication purposes may also be diminished, along with the ability to manage fraud and prevent the misuse of data though transaction monitoring if financial institutions do not have direct access to all customer financial transaction data and device information for this purpose.

Similarly, the current practice by TPPs to use financial institution log-in credentials to access customer financial transaction data leads to the mass storage by TPPs of financial institution log-in credentials and makes TPPs susceptible to financial crime. If a TPP has insufficient controls, there is a greater chance that cyber attacks will be successful, potentially resulting in fraud and losses to customers. Further, as financial institutions do not have a clear line of sight into the number of customers that have shared their online credentials with TPPs, a cyber attack on the TPP would be difficult to detect, contain, and manage.

The implementation of appropriate security controls by TPPs, and in particular the use of secure customer authentication, is a key requirement to managing the risks of data proliferation and increased connectivity associated with open banking. Further, APIs should continue to be developed to only allow access through secure communications protocols that facilitate communication between financial institutions' systems and TPPs without requiring customers to share their financial institution log-in credentials. Through an API, a TPP can access data without storing customer log-in credentials, by leveraging the financial institution’s robust authentication and authorization processes and reducing the risk of exposing customer log-in credentials. Moreover, to enable access via the financial institutions

dedicated API, the service allows the ability to turn off access at the customer's request or if there is a security concern. Most markets are converging on a specific API standard, and there is potential for the Canadian financial industry to do the same.

Naturally, there is more complexity around regulating the increased number of participants in an open banking system. With multiple new entrants, there could be disparity between the level of security and protection creating vulnerability to financial systems. While some of these requirements are covered by existing regulatory requirements under PIPEDA and could be dealt with through agreements with TPPs, there is also an opportunity for industry action to align on specific security standards that may be a more efficient and nimble means of ensuring adherence to the maintaining, processing, and sharing of customer data safely and securely.

Customers play an important role too. The security of a customer's financial transaction data is always paramount for financial institutions, and they invest heavily in protecting this data. Financial institutions are acutely aware of the ongoing threats to customer information, and are continuingly monitoring activities to defend and protect against them. While financial institutions have extensive security systems in place to protect customers from these threats, the government has a role to play in educating customers about the consequences of sharing their data with TPPs. Continued efforts on cyber security awareness are essential for customers to understand the steps required to protect themselves when participating in an open banking environment.

4. Financial Stability

As the Consultation Paper notes, consideration must also be given to risks to the safety, soundness, and stability of the overall financial system in Canada with TPP access to financial data in an open banking system. Canadians trust our financial system due to its stability, as evidenced by the banking industry's performance during the 2008-2009 financial crisis. As the federal government explores the merits of open banking, it is important to ensure that Canadian's trust in their financial system is not put at risk. The Financial Stability Board acknowledged the need to be careful about technology-enabled financial innovation when it wrote "while there is currently limited evidence regarding risks to financial stability

emanating from FinTech developments, change is occurring rapidly and decisions taken in this early stage may set important precedents"[3]. In principle, this perspective also applies to open banking since it is in the early stages of development and implementation in a number of international jurisdictions. Financial stability risk in this context should continue to be closely monitored.

Role of Federal Government

Canada has a long history as a global leader in developing industry solutions to help meet broad public policy objectives, through highly consultative and collaborative relationships between financial institutions and regulators. A scan of how open banking has been introduced and implemented in other jurisdictions demonstrates reliance on both industry and regulators, depending on the context of the policy drivers that gave rise to open banking in each jurisdiction and its existing legal and regulatory environment.

In some jurisdictions, financial authorities require banks to provide all accredited TPPs with access to a customer's data where the customer has provided the necessary consents. In such instances, the financial regulator oversees the management of risks and associated risk mitigants discussed in this submission, such as accreditation criteria and processes, appropriate liability frameworks, and mechanisms that facilitate TPPs' ability to fulfill their financial obligations to customers (e.g. professional indemnity insurance or comparable guarantees). In other jurisdictions, banks are working with other market participants, such as regulators, fintechs and data aggregators, to provide access to customer data with customer consent. These participants are working to enable secure data access by developing technical standards and best practices for authentication, consent, access and liability frameworks. Industry entities are being established to help drive potential efficiencies in the ecosystem by creating things like common technical and security standards and minimum accreditation criteria.

We have described in this submission the unique Canadian context, and the pertinent risks and possible solutions in our legal and regulatory environment, which should be taken into account when assessing how to proceed in Canada.

[3] Financial Stability Board, Financial Stability Implications from FinTech, Supervisory and Regulatory Issues that Merit Authorities' Attention, June 27, 2017. The Financial Stability Board defines FinTech as technologically-enabled financial innovation that could result in new business models, applications, processes or products with an associated material effect on financial markets and institutions and the provision of financial services.

Conclusion

The CBA strongly supports innovation and competition in the financial services sector, fueled by technological advancements. Given that both customer protection and the customer experience are central to banking, we have set out above the primary potential risks that would have to be mitigated in order for Canadian consumers and Canada's financial sector to truly benefit from open banking, as well as possible risk mitigants. As Finance Canada proceeds with its review of the merits of open banking, we welcome opportunities to continue to engage on these issues and gain a deeper understanding of the policy objectives underlying this review.