

Response to

“A Review into the Merits of Open Banking”

Department of Finance Canada,
February 2019

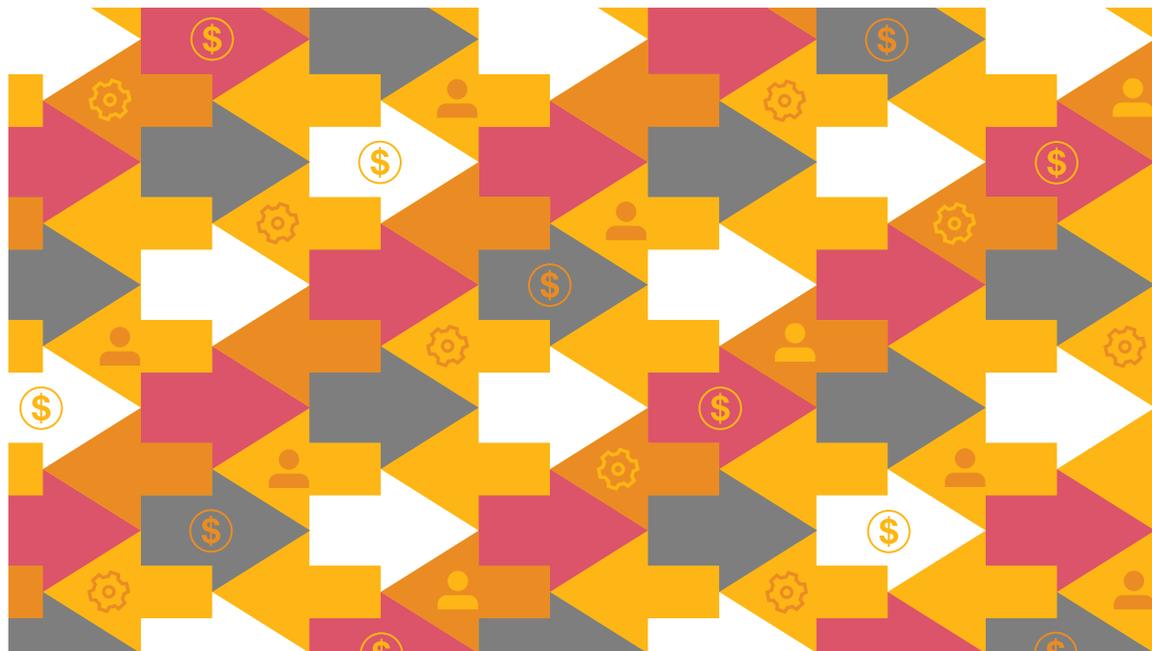


Table of Contents

Introduction	03
Benefits of open banking	03
Risk management considerations	04
Role of the federal government	07
Conclusion	09
Contacts	10

Introduction

PwC welcomes the opportunity to participate and provide commentary on the Department of Finance Canada's "A Review into the Merits of Open Banking" Consultation Document. Overall, we are supportive of an Open Banking framework in Canada and believe it will be an important and positive next step in modernizing the financial services industry.

Benefits of open banking

Would Open Banking provide meaningful benefits to and improve outcomes for Canadians? In what ways?

We believe that Open Banking will provide tangible benefits to consumers, foster competition in Canada's financial services sector, and accelerate innovation. Open Banking has the potential to transform the way consumers manage their finances by sharing their personal transaction data with other financial services providers.

To achieve this goal, a well-designed Open Banking system will need to place the consumer at the centre of the financial ecosystem. As consumer preferences continue to shift towards digital and personalized solutions, financial services providers will need to adapt to new ways of interacting with consumers. In today's world, maximizing customer engagement calls for creative, convenient, and proactive services that we believe can be better enabled through an Open Banking framework.

In addition to conventional consumers, the underbanked segment of the population can also benefit from Open Banking through the creation of new products and services that better cater to their specific circumstances. By allowing access to personal financial and transaction data, financial services providers can generate a more holistic financial picture of an individual, and provide access to services that would have otherwise not been available and that enhance the consumers' ability to manage their finances.

There are many potential applications of Open Banking. Participants could use transaction data to assess the credit worthiness of businesses and consumers beyond solely relying on traditional credit bureau checks or financial statements. Businesses and consumers could also allow their current provider to view their full transaction history from other financial institutions, and generate an aggregate view of their financial position for a variety of use cases. In addition, businesses could better integrate expense tracking and transaction data across financial institutions and third-party providers to help them with accounting activities and other areas of financial management.

These use cases are a sampling of potential applications, and we believe that Open Banking offers many possibilities to improve services and customer experience, ranging from more straightforward uses to a host of creative products and services that have yet to be imagined.

Open Banking will also generate greater competition in the financial services sector that will not only improve consumers' financial wellbeing, but also create a virtuous circle that would benefit the Canadian financial services ecosystem and the broader economy by benefiting all parties involved.

For new entrants, Open Banking will lower the barrier to entry and provide established and emerging financial technology companies (e.g. Fintechs) with easier means of accessing consumer data and parts of bank infrastructure (e.g. payment rails) without the need to resort to cumbersome and higher risk approaches such as "screen scraping" data from online banking portals.

For established institutions, greater access to consumer data from competitors can help develop a comprehensive consumer profile and enable better tailored products for both new and existing customers. In addition, a more vigorous banking ecosystem would create a universe of potential third-party providers, from both within and outside the financial services domain, which established banks could partner with for to bring new innovations to market.

This leads us to believe that as Open Banking opens the market to a wider range of market participants, consumers will be the overall beneficiaries as they will have a broader choice of products and services to meet their financial needs.

Risk management considerations

In order for Canadians to feel confident in an Open Banking system, how should risks related to consumer protection, privacy, cyber security and financial stability be managed?

Critical to enabling Open Banking is establishing the needed trust among all players in the ecosystem - consumers, participating financial institutions, regulators and emerging technology companies - in order to drive data sharing, innovation, and adoption.

Stakeholder trust has to be built on established privacy standards, robust security, and a consumer-focused strategy. This would apply to existing players as well as third-parties participating in an Open Banking ecosystem.

Stakeholder Trust =

privacy + security + being
perceived as acting in the
interests of consumers

Privacy

Financial institutions in Canada, and key players in the Open Banking ecosystem, are subject to PIPEDA (the *Personal Information Protection and Electronic Documents Act*). This law includes a core set of generally accepted privacy principles, such as accountability, purpose, access, openness, and accuracy - all important to bolster consumer trust. In addition to these baseline principles, a few others need to be considered as core components of any privacy standards to which the players in the Open Banking ecosystem are subject to:

- **A consent-based model** that is effectively enforced and puts the consumer in control. This means that consumer participation is subject to gaining explicit consent which can be easily revoked at any time at the consumer's discretion. Enabling consumers to participate in the ecosystem without any undue concern about their rights if they choose to discontinue their involvement with one, or more, providers for any reason at the future date.
- **Enhanced notice, transparency and controls** that provide consumers with clear and easy-to-understand notices of how and when their personal information will be collected, how it will be used, and with who it may be shared. According to a Harvard Business Review article¹, increasing transparency and control over how data is used and shared will drive consumers to share more data, provide more accurate data, and be more forgiving in the event of a breach.
- **"Privacy by Design"** that enables and drives the adoption of Open Banking by thinking strategically about privacy and ensuring that it is embedded into the design at the outset - a concept pioneered here in Canada by former Ontario Privacy Commissioner Ann Cavoukian² and enshrined into law in the European Union's General Data Protection Regulation (GDPR).
- **Individual personal information rights** that provides consumers with rights over their personal information, including the right to request access, correction and deletion of one's own personal information. Furthermore, it is worthwhile considering the introducing a right to data portability to allow moving of personal information between entities as part of the consumer's information rights, especially since PIPEDA already includes some of these rights while other jurisdictions have moved the dial on this topic. For example, the enhancements to these rights were enshrined in the EU's GDPR, and Australia has established the Consumer Data Right, which gives consumers formal ownership of their data in order to facilitate Open Banking with regards to certain product types.

The timing for this is rather opportune as PIPEDA is currently under review with several parties including from the Office of the Privacy Commissioner of Canada and the Standing Committee on Access to Information, Privacy and Ethics. Furthermore, the Ministry of

¹ "Research: A Strong Privacy Policy Can Save Your Company Millions", Martin, Borah and Palmatier, February 2018

² "PIPEDA Fair Information Principles", Office of the Privacy Commissioner of Canada, January 2018

Innovation, Science and Economic Development is examining this issue, including the exploration of the right structure for privacy that balances innovation enablement and privacy protection imperatives in a manner that promotes trust -- maximizing the potential of data and growing the digital ecosystem.

PIPEDA developments will directly inform the privacy, legal, regulatory, and policy requirements under which Open Banking will operate. It provides a foundation that is not only principle-based and technology-neutral, but also based on the core objectives of innovation and privacy protection. Having said that, the framework governing Open Banking may require further guidelines and standards (regulatory or otherwise) to effectively implement the above-mentioned principles.

Security

Given the nature of the data in question, effective standards for secure authentication must also be in place to ensure that access to consumers' sensitive financial data is protected in a manner that is not only appropriate to the nature of the data, but also to consumer expectations of a robust security framework. Multi-factor authentication, which requires the use of two or more pieces of evidence for authentication, fits the requirement for enhanced protection of consumer data in an Open Banking environment. Presently, two-factor authentication is a minimum requirement of both the UK's Open Banking initiative as well as the EU's second Payments Service Directive (PSD2). In addition, any framework must ensure that the data transferred to, and stored by, the new participants is secured to the standard that is comparable to one used by the banks.

To facilitate the interoperable and efficient exchange of data across Open Banking participants, Canada must establish technical API standards as part of its Open Banking framework. In addition to functional requirements germane to the Open Banking use cases under consideration, these standards must also focus on integrating security requirements into the API architecture and supporting tools in a manner that proactively addresses any incremental risks resulting from the access and transmission of data between the parties.

Another key consideration is enforcement, because standards are only reliable when backed up by effective monitoring and enforcement. To ensure that new entrants have implemented the standards for privacy and cybersecurity, Canada should consider establishing a certification process to screen participants prior to involvement in the Open Banking ecosystem. To promote transparency, the list of certified third-party Providers (TPPs) should be easily available to all consumers as a further security precaution. Furthermore, participants should be encouraged to further strengthen their respective third-party risk management programs to provide additional assurance on cybersecurity and privacy controls.

Finally, the framework for screening ecosystem participants must consider the stability (financial, operational, etc.) of the TPPs to further enhance consumer trust. This is a key consideration as the occurrence of one, or more, high profile events (e.g. bankruptcies,

outages, etc.) have the potential to undermine consumer confidence in the overall Open Banking ecosystem. This must be done in a manner that provides a baseline level of stability, but does not create unreasonably high barriers to entry, stifling innovation.

Acting in consumers' interest

“If you're not paying for the product, you're the product” is a common adage that has become increasingly popular in recent years to describe predominantly digital business models that offer some form of service to the consumers free of charge, while extracting economic value from the underlying consumer data in return.

In today's world, more data is available, and by extension there are new and innovative opportunities to use this data. While this creates many positive outcomes, it also creates new risks to companies, consumers, and regulators that need to be carefully considered.

Recent revelations about unintended inferences and surprising uses of data have increased scrutiny and enhanced societal expectations of companies to better account for consumer interests - in a way that not only meets the baseline legality threshold, but also passes the bar as being fair and responsible. These potential new uses of data create decision-making challenges, particularly from an ethical perspective, and reframes the question from “Can I use the data?” to “Should I use data in this way?”.

Consumers need to know that their interests are being considered as part of the trust equation. This requires both giving individuals more transparency and control over their data, as well as an evolved form of accountability, ethical processing, and data stewardship to help drive innovation while also reducing the risk of unintended consequences in the Open Banking environment.

Role of the federal government

If you are of the view that Canada should move forward with implementing an Open Banking system, what role and steps are appropriate for the federal government to take in the implementation of Open Banking?

We believe that the implementation of Open Banking in Canada would require the leadership of the Government of Canada from a policy and regulatory perspective. This is mainly due to the sensitive nature of the data and services involved, and the need to address any potential fraud, third-party, cybersecurity, and privacy risks that may compromise participants or undermine their confidence in the system. In addition, governments are generally better positioned to act as mediators between key stakeholder groups in a manner that balances their competing priorities with the greater public good.

To implement Open Banking in Canada, the federal government will need to consider a number of key questions, starting with how to effectively oversee its implementation in Canada. To this end, the government will need to decide whether to establish an implementation authority for the rollout of Open Banking in Canada, as has been the practice in other key jurisdictions, or whether to adopt a more hands-off role.

From a global perspective, we have observed that most comparable jurisdictions have adopted the hands-on approach. For example, the UK established an implementation authority, aptly named the Open Banking Implementation Entity (OBIE), with stakeholder representation from both businesses and individual consumers. The OBIE's mandate was to create software standards and establish industry guidelines on data exchange using APIs. OBIE was also responsible for defining security and messaging standards, as well as designing a process for managing complaints. OBIE is governed by the Competition and Markets Authority (CMA) in the UK, and was funded by UK financial institutions.

Similarly, the Australian Competition and Consumer Commission (ACCC) acts as a body to monitor implementation of Open Banking, and consults with other bodies to ensure correct privacy, escalations, and enforcement procedures are adhered to. In collaboration with Data61 (Australia's digital innovation arm of the national science agency), they are responsible for governance of the Consumer Data Right and the development of standards.

We believe that it would be beneficial to follow the central implementation authority model, as has already been done in other countries, in order to proceed with Open Banking in a secure and structured manner. To this end, the government will need to define the mandate of the authority, and whether it would be responsible for establishing standards, or simply monitoring the implementation of those standards. To further safeguard the Canadian financial system, the implementation authority should also be involved in the design of the dispute resolution processes needed to resolve potential consumer complaints, as well as acting on any cases where applicable policies may have been circumvented.

Any framework for the Canadian ecosystem must also address a rather uniquely Canadian challenge that is the degree of jurisdictional fragmentation. Given that Canada does not have a single regulator and/or jurisdiction to oversee the financial services sector, special consideration will need to be given to how Open Banking regulations are aligned, managed, and enforced consistently across the country.

Depending on the implementation framework selected for Canada, it is imperative that the implementation body drives a coordinated effort across federal (e.g. OSC, OSFI, CMHC, and Payments Canada) and provincial regulatory bodies (e.g. provincial regulation of credit unions, securities). The federal government must also define the criteria for participation in the Open Banking network, which products would be in scope (e.g. deposit, lending, etc.), and drive consensus on whether to execute based on a full or phased implementation timeline. In addition, the federal government should consider the appropriate means of extending regulatory coverage to new participants who do not fall under current frameworks to ensure that an appropriate level of oversight is maintained. Another key consideration is

achieving “regulatory parity”, which we define as striking a balance that would encourage experimentation and innovation, without disadvantaging the established financial institutions who may find themselves constrained by legacy regulatory frameworks.

In a similar vein, the federal government will also need to consider the adoption of an API specification and certification standard that would simplify interoperability across jurisdictional boundaries (e.g. banks and credit unions) or industry segments (e.g. banking and wealth management). A highly interoperable Open Banking environment would require national API standards, which has been the practice in other jurisdictions. As part of this effort, the design will also need to address the question of consumer identification and authentication standards to prevent identity theft and/or mitigate potential fraud risk.

For example, the UK OBIE has adopted a certification program with the OpenID Foundation known as Financial-grade API to enable future participation on the Open Banking network. This can also be seen in other jurisdictions, where there is a strong emphasis on common API infrastructure and harmonized technical standards as a systematic design feature.

We believe that adopting a common standard is in the best interest of the industry, as it will allow financial institutions to focus on customer experience and product innovation, rather than having to develop and integrate a universe of proprietary API systems which would be costly, and could add additional barriers for market entrants.

Finally, shaping public perception of Open Banking is another critical role for the government. This means ensuring there is adequate consumer awareness, education, and imperatives to encourage individuals to modify current habits. As was seen in the UK, initial adoption was limited due to a lack of Open Banking awareness among UK consumers. A proactive approach in Canada will help with consumer and business attitudes towards Open Banking.

Conclusion

Open Banking has the potential to revolutionize the Canadian financial landscape. With careful consideration of the risks and role of the government in its implementation, Open Banking can bring a new era of competitiveness and innovation to financial services in Canada and around the world.

Contacts

For questions regarding this submission, please contact:

Paula Pereira

Partner, Banking and Capital Markets, Consulting Leader
+1 416 941 8460
paula.x.pereira@pwc.com

Sasan Parhizgari

Senior Director, Consulting & Deals
+1 416 947 8903
sasan.parhizgari@pwc.com

Naren Kalyanaraman

Senior Director, Financial Services Cyber Leader
+1 416 815 5306
naren.x.kalyanaraman@pwc.com

Jordan Prokopy

Director, National Privacy Practice Leader
+1 416 869 2384
jordan.prokopy@pwc.com

pwc.com/ca

© 2019 PricewaterhouseCoopers LLP, an Ontario limited liability partnership. All rights reserved. PwC refers to the Canadian member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.