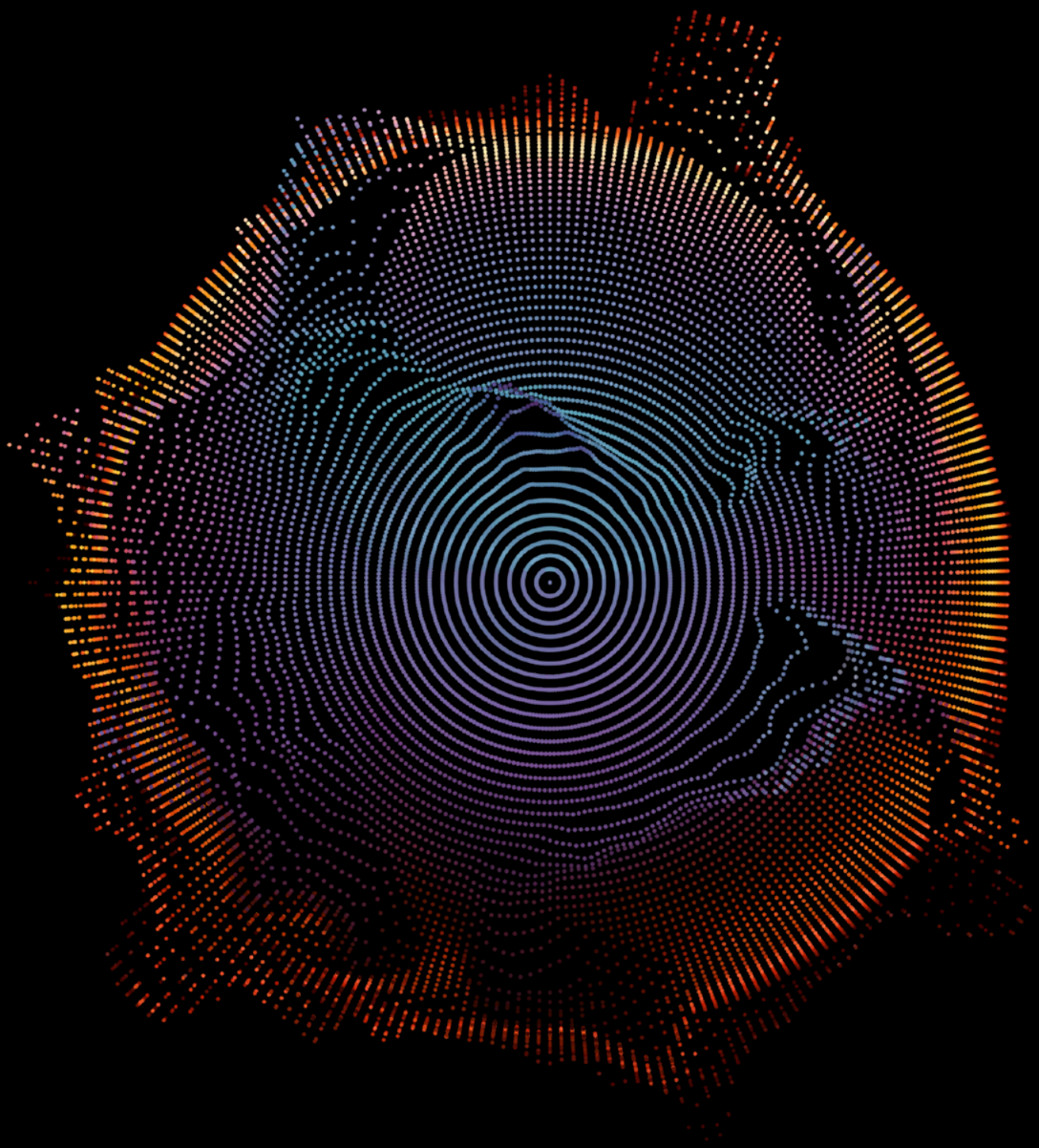
Deloitte.



Creating an open banking framework for Canada

Considerations and implications of key design choices

Contents

Executive summary

As the strategic importance of data grows in the digital economy, various models of enabling customers to share their personal data with third-party organizations are proliferating in the financial services industry. Building on the principles of customer control and portability of their personal data, many global or industry-led open banking data access models over the past five years to address the shortcomings of current data access models and accelerate data-driven innovations.

Enabling customers to share their personal financial data with trusted third parties has a potential to deliver improvements and new value in financial services—from digital advice to financial automation to new products. However, widening access to the sensitive data without proper safeguards can also introduce new risks to the financial system, eroding the new value generated.

Canada is renowned for its ability to uphold financial safety and stability. As the initial discussions on open banking progress over the next few years, Canada has a unique opportunity to design a third-party data access model that delivers ultimate value to customers by balancing innovation and competition with preservation of systemic resilience.

Creating an open banking framework for Canada | Executive summary

To do so, Canada must contemplate on the ultimate objectives of open banking and reflect them, as well as unique characteristics of the Canadian financial services landscape, to the design of the data access framework. In particular, throughout this design process, stakeholders will have to find answers to three key questions:

1. Scope

What type of data and which institutions should be part of the framework?

2. Standardization

How centralized and standardized should governance, data sharing, and authentication be?

3. Commercial and liability model

How should interactions between data generators and data consumers be structured?

This paper is designed to help stakeholders consider the implications of these choices by analyzing decisions made by other jurisdictions, enabling them to establish an open banking framework that works for Canadians. It is our belief that by effectively framing the dialogue—and learning from the experiences of other jurisdictions—Canada not only has the ability to embrace the benefits of open banking, but establish a blueprint for a truly digital economy as well.

Introduction

What is open banking?

Open banking is a global movement that promotes a customer's right to share financial information with third parties.

While many global jurisdictions have legislated open banking policies, open banking is broader than just policy—it's a movement comprised of technical, competitive, and regulatory shifts to help customers regain control of their own data and make it more portable between institutions.

Open banking policies in some jurisdictions dictate openness in both data access and payment initiation activities. In this paper, we focus primarily on laying out Canadian considerations for data access or the "account information" portion of open banking policies rather than payment initiation.

Driving forces of the open banking movement

The rise of the fourth industrial revolution has been marked by the emergence of companies that leverage data to deliver value. The rising importance of data has bolstered the value customers, businesses, and governments assign to data and in turn has sparked deeper contemplation on who ultimately has the right to control it. As a result, many now believe customers have a right to control their personal data that is held by various organizations—including being able to share it with third parties of their desire. This philosophy is deeply embedded in the modernization of privacy laws, such as the General Data Protection Regulation (GDPR) in the EU and proposed changes to the Personal Information Protection and Electronic Documents Act (PIPEDA) by the House of Commons in Canada.

It is not a coincidence that various models of data sharing have emerged over the past two decades in the financial services industry, which generate and process a vast amount of personal data, to meet growing customer demand for data sharing. However, many of these practices have inherent shortcomings that present trade-offs across security, interoperability, and accessibility. Over the past few years, regional efforts to create a harmonized approach to enable data sharing while addressing these challenges have resulted in both regulatory actions and industry-driven collaborations in various jurisdictions around the world—efforts that Canada can learn from.

This paper aims to discuss the key choices that define an open banking framework and their downstream implications, independent of whether the framework is driven by a policy or by the market participants.

Current data-sharing methods in financial services

A variety of mechanisms are used today to facilitate the sharing of customers' financial data, such as CSV downloads, extract transform load (i.e., "screen scraping"), and bilateral data-sharing partnerships. To develop an effective open banking framework, it is therefore important to first understand the movement as the evolution of these data-sharing models.

CSV

From the onset of online banking, most financial institutions offered customers the opportunity to download their transaction data through online portals in a commonly analyzable CSV file format that can be shared with other providers. However, this method comes with its fair share of challenges—most notably, it is often cumbersome for customers, not ideal for repeated data sharing, inconsistent across institutions, and often limited to transaction data. Most importantly, this method of data sharing lacks security measures to protect the data, creating opportunities for data manipulation.

Extract transform load (ETL)

Often called "screen scraping", ETL practices were first developed to address customer pain points associated with CSV file sharing. ETL providers enable a customer-approved third party to use users' online banking credentials to log into financial institutions' online portals and "scrape" or extract the data from the portals. These providers then reconcile, enrich, and transform the extracted data and load the newly formatted information into the third party's database.

In many financial markets, particularly in the US, the growth of ETL has fueled many early innovative use cases of data sharing—from the evolution of personal financial managers to enriched accounting dashboards for small businesses. While this method reduces customer friction, it introduces many additional security concerns, including those related to the storage of customers' online banking credentials, lack of ability to enforce informed consent, unclear liability responsibilities, and storage of data gathered by ETL providers. Because of these risks, many financial institutions are putting temporary measures into place to block ETL access, resulting in issues around data availability and increased costs to maintain connectivity. In fact, these risks are so great that ETL is being banned in some existing open banking markets—but only for the institutions and types of data subject to open banking.

Bilateral data sharing

To address security and operational concerns with screen scraping, many global financial institutions have formed more controlled one-to-one data-sharing partnerships, either directly with third-party providers or with ETL providers. In most cases, these partnerships replace unsecure credential capture and online platform access with API-based authentication and data sharing supported by formalized commercial and liability terms. However, because they are mostly conducted on a one-to-one basis, these closed data-sharing partnerships are not scalable and are often limited to the largest data consuming organizations, such as digital accounting platforms.

The next phase of data sharing

The development of a harmonized and agreed-upon open banking framework enhances the process of data sharing in a number of ways:

- **Increased interoperability:** Driven by the widespread adoption of standardized data-sharing protocols and guidelines, open banking makes it easier for third parties to access customer data and deliver more value to customers.
- **Greater reliability and security:** Open banking provides a safer and more stable alternative to current data-sharing practices.
- **Clearly defined standards on issues such as liability:** Open banking has the potential to increase confidence and participation in the data-sharing ecosystem—both on the part of customers (concerned about the misuse of their data) and financial institutions (concerned about new liabilities and reputational risks posed by third parties).
- **Improved accessibility:** Open banking materially reduces the cost of data sharing among financial services organizations through the establishment of open APIs and the transfer of data control to the customer.

In designing the open banking framework for Canada, it is important to note that open, harmonized data sharing exists within an evolutionary spectrum along with these other methods of sharing data. Even with the introduction of Open Banking, these methods of data sharing will continue to exist to fill in the gaps.

Open data and the future of financial services

By offering broader access to customer data, open banking not only has the potential to create a more competitive and innovative financial services industry, but, combined with other industry shifts, like streamlined payments infrastructure, artificial intelligence (AI), and an influx of non-traditional players, it has the potential to make broader shifts to the economy as a whole.

Below are just a few ways open banking could change the face of the Canadian financial sector:

Emergence of central interfaces
Today, financial product providers are the controllers of customers' financial data, largely because these companies own the digital interfaces. For individuals that work with more than one financial institution, this can be inconvenient as it causes fragmented visibility into their financial portfolio.

By allowing trusted third parties to gain access to customers' financial data, open banking enables certain players to act as a central interface by linking information from multiple financial and adjacent product manufacturers. This disaggregation of the financial services value chain could change how Canadians access and manage their financial information. For instance, without today's existing roadblocks separating financial product distributors from manufacturers, digital personal finance management tools and accounting platforms could enhance the quality and scope of their interfaces.

Proliferation of digital advice
As the central financial interface evolves, the value the interface needs to provide increases to captivate customers. Advances in machine intelligence, faster payment vehicles, and broader access to customer data will allow online financial platforms to offer more than merely an aggregated display of information and instead provide more active digital financial advice.

There are signs this is starting to happen. Many personal finance management tools are already moving into subscription management and product comparison, such as Bean in the UK and Clarity Money in the US. As open banking matures, these offerings may further evolve to enable next-best action recommendations and near-total automation of finance management.

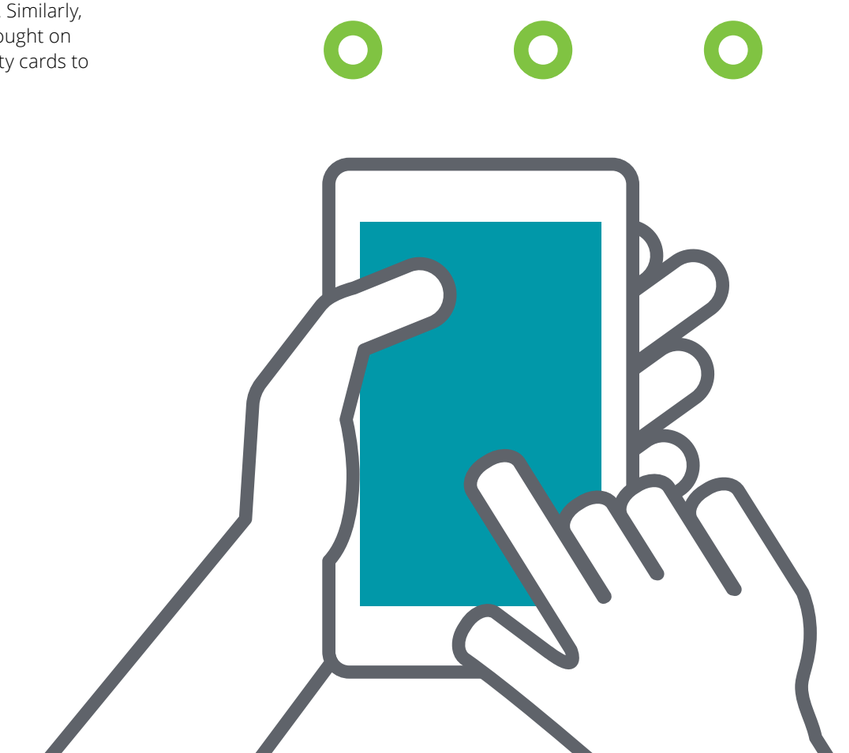
Lower barriers to play
The emergence of central interfaces will present unique opportunities for non-traditional players, including retailers, global financial institutions, large technology companies, and fintechs. Without the regulatory burden of providing deposit accounts, these players can more easily participate in the banking value chain and will likely leverage their new market position by becoming central interfaces themselves, relying on a third-party product shelf. As a result, the organizations that will have protected proprietary data—such as retailers with access to transaction information or large technology companies with access to user preference information—may gain an advantage against traditional financial institutions. Others will participate in the market as providers of investment and lending products by working with central interfaces.

Creating an open banking framework for Canada | Introduction

Intensified product-level competition
The proliferation of central interfaces will allow customers to gain better visibility into alternative financial products, compare them, and switch providers without foregoing the main relationship with the central interface. It will also allow for the needs-based substitution of traditional products, such as replacing long-term deposits with money market funds, for instance.

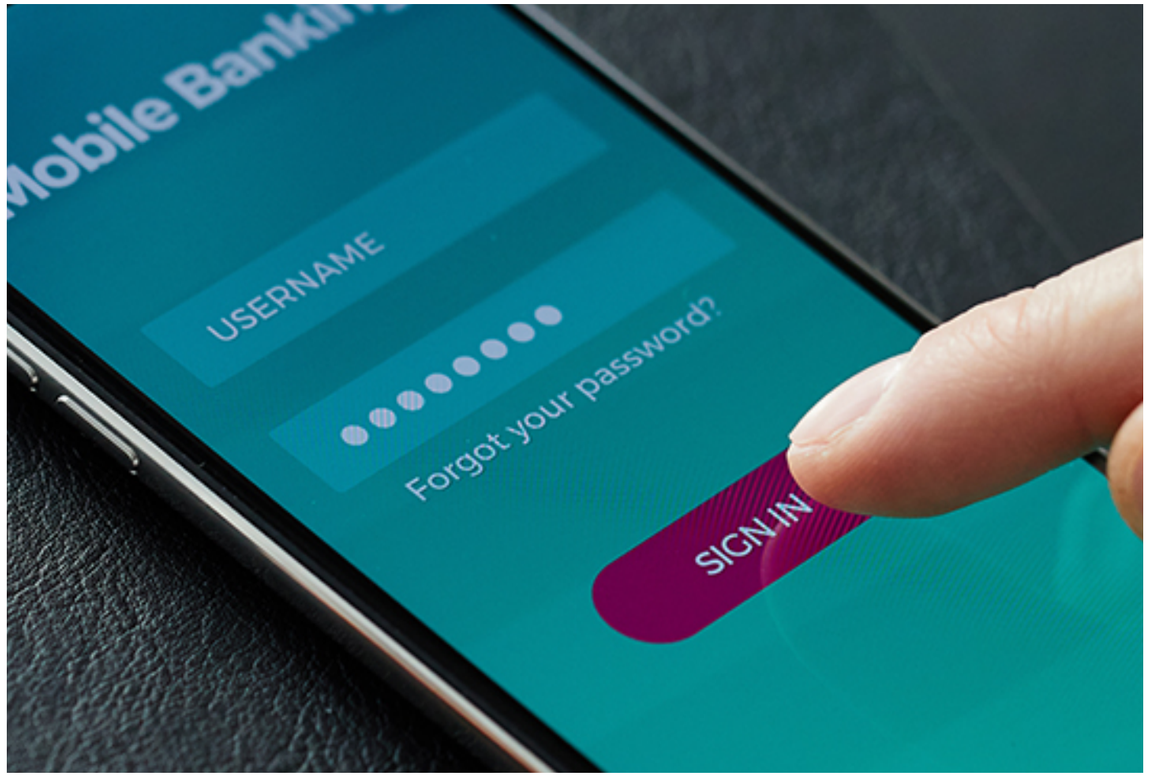
Products on top of products
Near-real-time visibility of customers' financial transactions will also allow for the development of innovative products that can be bought on top of existing products. For instance, digital installment loan products may be bought on top of existing debit and credit cards to provide a more sustainable borrowing option. Similarly, warranty insurance may be bought on top of purchases on third-party cards to provide flexibility.

Granularized loan adjudication
Increased access to individual, transactional data will allow lenders to better understand customers' risk profiles at a more granular level. Lenders will be able to augment credit scores with empirical cash flow data to better understand individual customers who do not currently hold relationships with them. Furthermore, lenders will be able to price risks for each individual transaction to reflect its context, from purchase type to total borrowed amount.



Open banking and emerging risks

While open banking offers countless opportunities for the financial services industry, it's clear the subsequent growth of data-sharing practices with third parties will also open our financial system up to a new host of risks. To preserve the safety and soundness of our financial ecosystem, An open banking framework must not only proactively identify these new risks, but take steps to mitigate them.



Creating an open banking framework for Canada | Introduction

This will require asking a variety of difficult questions:

New entrants

How will their activities be governed to ensure customer and ecosystem protection and control measures are in place?

Open banking allows "product light" non-traditional participants to enter the financial services value chain without becoming fully licensed banks or financial institutions.

Data breaches

How will we ensure the data shared among ecosystem participants remains secure?

As customer data is distributed across a larger number of industry players (with potentially different standards for data security), organizations will become more vulnerable to malicious third parties as well as mistakes, increasing the likelihood of cyberattacks and inadvertent data leaks.

Fraud

How will we ensure the ecosystem is not exposed to fraudulent third parties?

As the number of interactions increases across ecosystem participants in an open framework, the opportunities for fraudulent third parties to engage in phishing activities and access customers' personally identifiable information may increase.

Privacy

What improvements to privacy measures will be required to properly protect customers' data?

For open banking to work effectively, customers must not only be educated and informed, but they must also consent to how their data is used. Without the proper mechanisms in place, customers' private information may be used for purposes that are against their interests.

Recourse

How will the open banking ecosystem be operationalized to effectively deal with liabilities while minimizing customers' exposure?

A distributed data landscape will make it increasingly difficult to seek recourse following a breach, fraudulent event, or other cybersecurity incident, potentially creating a shortfall in customer support.

Distribution of costs

How will the open banking system collectively address the efforts associated with open banking to incentivize all parties to proactively participate?

Setting up and operating a more secure data-sharing mechanism will cost both individual institutions and the overall financial system substantial amounts of resources (up to $200M for a leading Australian bank[1]). If open banking increases the volume of data-sharing practices by customers as intended, the cost of maintaining the system will also grow. Without fairly distributing these costs, the benefit of open banking might be offset by these added costs passed on to customers.

A prudent open banking framework will not only recognize these emerging risks, but will also establish a strong supporting regulatory environment to mitigate them—one that includes, among many things, robust financial governance frameworks and privacy regulations. This foundational step is critical because, without carefully managing potential risks associated with open banking, the net benefit of and participation in an open data landscape will diminish.

Considerations for a Canadian open banking framework

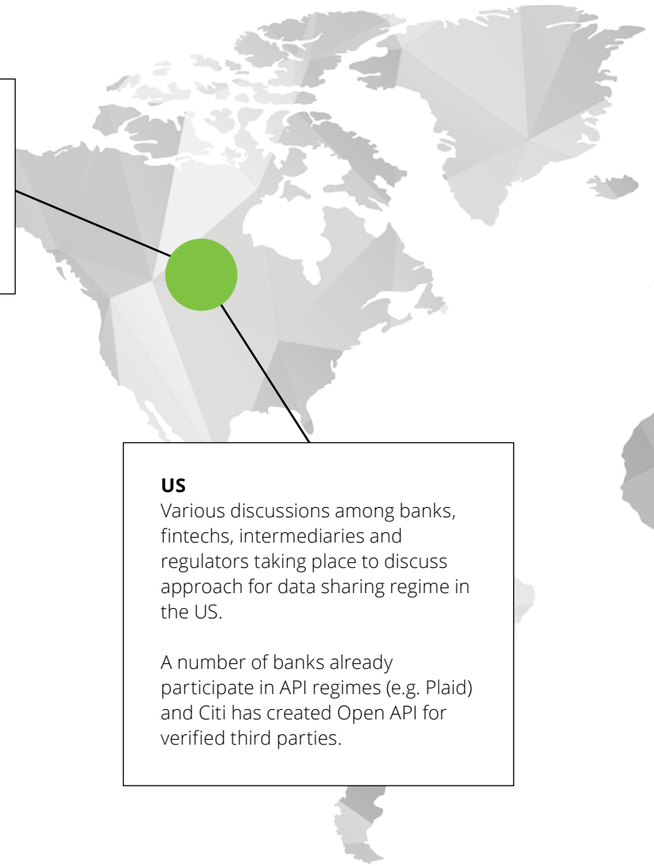
Global precedents

Given that countless jurisdictions across the world have already adopted open banking, there are many examples for Canada to pull from when establishing its own framework. That being said, because every country has different banking systems and circumstances, there is far from a standard design; in fact, those that already exist feature a high degree of variation in policy and design choices.

Creating an open banking framework for Canada | Considerations for a Canadian open banking framework

A number of jurisdictions across the globe have begun to implement Open Banking policies, each finding themselves at varying stages of maturity.

Canada
Regulators have begun discussing open banking as part of the 2018 federal budget. An advisory committee on open banking was established in September 2018, and the consultation process began in January 2019 with the release of a consultation paper.



US
Various discussions among banks, fintechs, intermediaries and regulators taking place to discuss approach for data sharing regime in the US.

A number of banks already participate in API regimes (e.g. Plaid) and Citi has created Open API for verified third parties.

UK: CMA
Requires nine identified banks to share banking data and payment initiation through open API standards.
Effective January 2018

Japan: Open API
Banks in Japan are required to announce support on open API by March 2018 for deployment by 2020. Third-party service providers are required to register and establish contracts with banks.

Hong Kong: Open API
HKMA issued a consultation paper in January 2018 setting out its intended approach to open APIs as part of the "New Era of Smart Banking."

Singapore: Open API
As part of building a "Smart Nation", the Monetary Authority of Singapore (MAS) and the Association of Banks in Singapore (ABS) issued an Open-API playbook to encourage financial institutions to develop and share their APIs openly.

EU: PSD2
Requires banks to share banking data and payment initiation, but technology neutral.
Effective January 2019

Australia: Consumer data right
New legislation announced in November 2017 will grant consumers open access to their banking, energy, phone, and internet data. Banking is the first industry that will be subject to this new legislation.
Effective 2019

4 global approaches to open banking

America
Laissez-faire approach to regulation; screen-scraping predominant.

Asia
Reliance on institutions to drive open banking innovation; supportive, rules-light regulatory environment.

Europe
Open banking borne out of payments legislation and desire to harmonize legislation.

Australia
Rules-driven approach; banking simply one of a broader push to develop a data economy.

United Kingdom

In the UK, open banking regulation was driven by a policy objective to decrease the market power of the largest banks by increasing the range of service providers in the market. In its 2016 Retail Banking Market Investigation, the Competition and Markets Authority concluded that "older and larger banks do not have to compete hard enough for customers' business, and smaller and newer banks find it difficult to grow. This means that many people are paying more than they should and are not benefiting from new services."[2] As a result, the UK's open banking framework focuses only on the largest nine banks without any reciprocity.

Australia

In Australia, open banking regulation was adopted in response to growing public scrutiny of large banks, and aims to empower customers with the right to control and benefit from their data. The government's review into open banking identified it as a useful tool in "providing customers with better access to financial data and reduces the time, cost and inconvenience associated with identifying and selecting financial products and services. When consumers make better choices about how and what to consume, the industry affected is driven to become more efficient and competitive."[3] The movement extends beyond financial services and is part of the country's broader Customer Data Right ambition to create an open data economy. Over time, this open data regime, similar to open banking, is expected to eventually encompass other industries, starting with telecom and utilities. Because of this vision, Australia's open banking policy is broad and all encompassing, requiring all deposit-taking institutions—not just banks—to participate, and covering both digital and physical channels, for example.

Japan

In Japan, the open banking movement was driven by a policy objective to promote innovation and modernization in the banking industry as part of the Japanese government's 2017 Growth Strategy[4]. In Japan, there is a perception among key regulatory and government stakeholders that the nation's financial services sector is lagging behind other jurisdictions, making it more susceptible to the effects of potential exogenous shocks and affecting its global competitiveness. Furthermore, a heavy reliance on cash payments and historically strict regulatory practices (e.g., limiting banks' abilities to take sizeable equity stakes in fintechs) have stifled the innovative capacity of the sector. Open banking and the regulatory modernization that will accompany it (including a relaxation of investment limitations with respect to fintechs) are seen as key tools to increase growth, drive competitiveness, and promote innovation.

European Union

In the EU, the objectives of the open banking policy are to better harmonize the fragmented payment sector, modernize the financial sector, and provide customers with alternatives to big banks that were involved in systemic failure. The EU has chosen to take a distinctly activity-based approach to regulation (by regulating payment services as a whole vs. specific types of institutions) and has put particular emphasis on applying consistent technical standards, especially those focused on improving security (e.g., authentication and communication). This focus on regulating activities and promoting technical standardization can be seen as a direct result of the EU's unique market structure; thousands of payment providers of various sizes and levels of sophistication are domiciled across 28 Member States, each with its own unique regulatory and market context. The key piece of legislation driving the open banking initiative—Payment Services Directive 2, or PSD2—expands the scope of previous legislation to cover a greater breadth of transactions, ensure consistent application across Member States, and provide third-party access to customer payment data. It also broadens the range of eligible payment service providers (thereby encouraging innovation) by easing market entry for new providers, while ensuring consumer protection through improved standards.

United States

In the US, there is no imminent regulatory driver to open banking; however, various market participants—including regulators, trade associations, financial institutions, and data aggregators—are publishing standards and perspectives on a potential data-sharing model across the industry. For instance, the Consumer Financial Protection Bureau (CFPB), a consumer protection watchdog for the financial industry, has published a set of non-binding principles focused on financial data sharing and aggregation, while the National Automated Clearing House Association (NACHA), a financial industry association, has convened an API Standardization Industry Group to develop consistent API standards for the financial services sector. A number of prominent fintechs (including Betterment and Kabbage) have also joined forces to create a lobbying group, the Consumer Financial Data Rights group, to promote the sharing of consumer financial data with third parties.

Creating an open banking framework for Canada | Considerations for a Canadian open banking framework

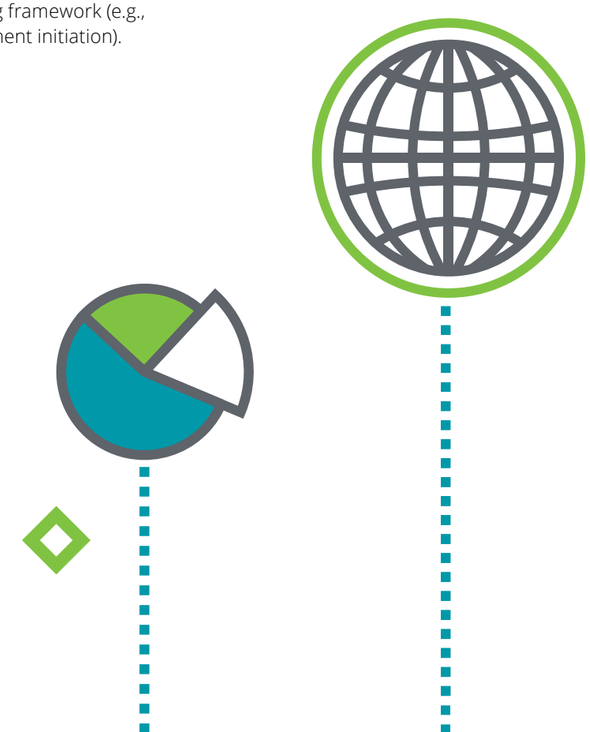
Singapore

The Monetary Authority of Singapore (MAS), the city-state's central bank and a highly progressive advocate of innovation in financial services, has cultivated a robust open banking ecosystem without developing mandatory legislation governing third-party data access. In part, this is due to Singapore's unique market conditions. Strong competition in the banking sector has seen the nation's largest financial institutions, including DBS and OCBC Bank, take a proactive approach to innovation and be among the first to experiment with Open API technology. Indeed, today they are global leaders in terms of data sharing; DBS, for instance, provides developer access to over 200 APIs, covering products and services such as payment cards, rewards, and loans. The MAS also maintains a strong and highly collaborative relationship with Singaporean banks, which lessens the need for prescriptive legislation to achieve certain market outcomes. An example of this collaboration, as well as the central bank's progressive outlook on the banking industry, is Singapore's API Playbook, which developed jointly between the MAS and the Association of Banks in Singapore. The Playbook contains over 400 recommended APIs for banks to develop, stretching far beyond the scope of open banking (i.e., third-party data access) to cover all aspects of the banking value chain, from front end to back end.

The Canadian context

A Canadian open banking framework should be purposefully designed based on Canada's unique characteristics. Specifically, it should consider:

- A sound financial services system that has not experienced systemic failure or relied on public funding.
- A bifurcated regulatory landscape where federal and provincial bodies govern different entities, but with a manageable number of institutions. This creates complexity in developing standardized approaches and governing open banking participants (compared to jurisdictions with central oversight).
- Lack of governance for non-traditional entities that do not fit into existing definitions of "financial institutions", which may expose customers to new sources of risk without protection, or expose the financial services ecosystem to foreign institutions.
- Ongoing efforts to strengthen Canadian privacy legislation through proposed amendments to the PIPEDA, which would act as guardrails for An open banking framework on the permitted usage, data management, and disclosure requirements.
- Ongoing payments modernization efforts to enhance Canadian payments infrastructure, which may help facilitate the building of An open banking framework (e.g., third-party payment initiation).



Creating an open banking framework for Canada | Considerations for a Canadian open banking framework

As a result of these unique circumstances, open banking in Canada should:

Focus on delivering value to Canadians
Open banking presents an opportunity to develop a governance framework for non-traditional financial services providers (in conjunction with other concurrent efforts in Canada) and to spur innovation.

Increase transparency and customer control of data
Open banking should be a broad, industry-agnostic movement that focuses on placing the control of data back in the hands of customers.

Mitigate data-sharing risks
Current financial data-sharing methods threaten the safety and stability of the financial services system by requiring customers to share their banking credentials with third parties.

Preserve our stable financial services system
Punitive intent against specific institutions should not be a key objective of open banking.

These unique objectives indicate that the design of an open banking framework in Canada should differ from those observed in other geographies. While certain elements may be transferable, Canada should strive to develop an open banking infrastructure from the ground up, with the country's specific circumstances in mind.

Design principles for an open banking framework

In its 2018 budget, the Government of Canada said it would review the merits of open banking to assess whether the movement would deliver "positive results" for Canadians. But what are "positive results"? The answer to this question is two-fold.

On the one hand, a successful open banking framework should support the continued evolution of innovation within the financial services ecosystem. On the other, open banking should continue to protect, maintain, and bolster the safety and soundness of Canada's renowned financial system.

To generate these types of results, Canada must focus on several key guiding principles when designing its open banking system:

1. Value:
Focus on delivering true value to Canadians without placing undue burdens on any participant (e.g., of cost, risk exposure).

2. Transparency:
Ensure customers are fully informed of their rights and responsibilities regarding the transfer, possession, and use of their data.

3. Safety:
Balance customer convenience with safety and security.

4. Adoption:
Balance the net cost to the economy, participation, and speed to market with the scope of products and/or data.

While there are countless factors to keep in mind as we move forward with an open banking framework in Canada, these four guiding principles should be the cornerstone on which all decisions are based.

An open banking framework for Canada

Framework overview

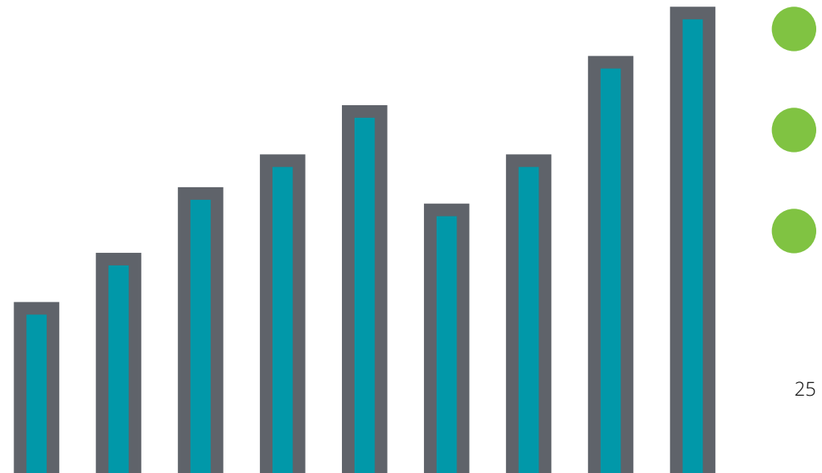
To build an effective Canadian open banking framework, stakeholders must consider the choices and outcomes observed in other jurisdictions and weigh them against Canada's unique context.

The design of open banking can be categorized into three key decision areas:

1. Scope of open banking

2. Standards

3. Commercial and liability model



1. Scope of open banking

The choices made by other jurisdictions around the scope of open banking help define the types of accounts and entities from which open banking will mandate data access, how this access might change over time, and methods by which this data can be accessed.

While building an open banking framework, Canada should answer these questions:

- What products should be covered?
- Should "offline" accounts be covered?
- Which types of users should be covered?
- Which types of data should be included?
- How far back should data be made available?
- Who should be required to open access to their data?
- How should the rollout work?
- Which types of data recipients will be allowed?
- What access rights should data recipients have?

What products should be covered?

Choices made by other jurisdictions:

One of the first steps in establishing an open banking framework is to determine the types of financial products it should encompass. To date, most open banking systems focus on three core areas:

1. Transaction accounts
Examples: Debit, credit, savings
Impact of open banking: Allow for more personal financial management and adjudication use cases.

2. Savings/lending products
Examples: GICs, TFSAs, mortgages, LOCs
Impact of open banking: Allow for seamless product switching and comparison use cases.

3. Broader financial products
Examples: Wealth and insurance products
Impact of open banking: Allow for more holistic financial management use cases.

Ideally, open banking has the potential to both increase the breadth of products available in the marketplace and generate a broader scope of use cases. That being said, achieving this end goal is not without its challenges, and the products Canada chooses to include in its framework will require careful consideration.

For instance, certain financial products—such as wealth and insurance products—will inevitably create additional burdens for data generators as they strive to make data available to third parties. Unlike transaction accounts, which are updated on a continuous basis, these products may not be fully digitized, or may require new forms of online access. This could result in expensive and time-consuming system restructuring.

A Canadian open banking framework also must have a clearly defined scope. This means stakeholders will have to decide whether to regulate functions on a product-based approach (which defines specific types of accounts in and out of scope) or an activity-based approach (which defines specific actions that are in and out of scope). An activity-based approach has the benefit of more fairly requiring participation from institutions, but it needs to be clearly defined if regulators hope to prevent confusion around which institutions are in scope and which are not.

Of those jurisdictions that have already adopted open banking, the UK and Australia have taken an account-based approach, while the EU defines its scope on an activity basis (e.g., "all online payment accounts"). Like the UK and Australia, the EU's definition includes chequing accounts, credit cards, etc., but also may include other comparable accounts such as online wallets (e.g., PayPal).

Should “offline” accounts be covered?

Choices made by other jurisdictions:

Should a Canadian open banking framework only include online financial products, or should “offline” accounts also be in scope? To find the answer to this question, we must look at two key factors:

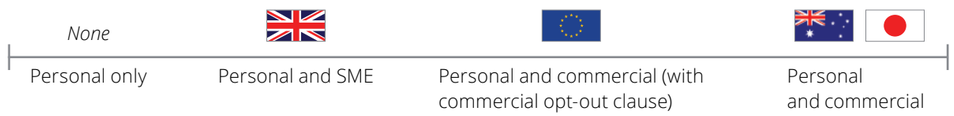
1. Scope of customers:
As of 2016, 90 percent of Canadians had regular access to the internet, and 80 percent used some form of online banking—a number that is expected to increase over time.[5] This means that, since open banking will most likely be delivered through digital means, the majority of Canadians will have access to it, but not all. By ignoring those customers without online banking access, open banking would inevitably be excluding society’s most vulnerable, most notably, the elderly and low-income Canadians.

2. Scope of work:
For offline products to work with open banking, institutions would have to make existing data available digitally—an effort that would not only require the building of digital processes, but also the onboarding of customers to an online platform to simplify authentication. While this would ensure all Canadians had access to open banking, it would inevitably increase the cost and complexity of implementation, resulting in a longer timeline to launch.

Developing a deeper understanding of how many Canadians would be involuntarily excluded from open banking if non-digital data is excluded from the scope, as well as the unique needs of those Canadians, is crucial to understanding if the additional complexity and cost to financial institutions is justified.

Personal versus commercial: Which types of users should be covered?

Choices made by other jurisdictions:



For each type of user, there exists a tradeoff between implementation cost and complexity, and value to consumers. Currently, different users are afforded different levels of service: retail (i.e., personal) account holders receive largely off-the-shelf products and services, while large corporate account holders already enjoy some of the benefits that new solutions under open banking would support (e.g., individualized cash flow management and advice). Those customers using small business banking accounts (small-to-medium sized enterprises, or SMEs), on the other hand, receive a mix of off-the-shelf and easily customized offerings, as befits their position between retail and large corporate customers.

Also, different types of user accounts have different levels of digital access and integration (i.e., API-led or bespoke integrations). Personal accounts have largely been digitized around the world, and customers can usually view most-to-all of their accounts and products at one institution through a single web or mobile portal, making opening up access to that data through APIs relatively straightforward. However, for corporate accounts, the degree to which banks have built single points of access for a firm’s products and funds is highly variable. Because of this, applying open banking to the breadth of a firm’s corporate accounts may be a technological challenge as well as a regulatory one.

From a global perspective, the vast majority of open banking initiatives and regulations have been focused on retail and SME use cases. This is primarily because technical implementation for these users is often easier and democratizing data for retail customers is more closely aligned with most countries’ catalysts for open banking. However, Australia has included a provision in its open banking framework to open it up to all accounts—including commercial—although the details have yet to be finalized by the Australia Competition and Consumer Commission (ACCC).

Which types of data should be included?

Choices made by other jurisdictions:

Public data

Customer-generated data

Balance data

Choices made by other jurisdictions:

Transaction data

Identity verification data

Aggregated data

Based on a review of the total scope of data access in other jurisdictions, a number of types of data can be identified:

- **Public data:** Information that is readily accessible online and can be freely used, reused, and redistributed by any entity (e.g., customer reviews and publicly available product information). In Canada, much of this information is already accessible through other data-sharing ecosystems (e.g., Google, Yelp, and Foursquare APIs).
- **Customer-generated data:** Personal and financial information provided directly by the customer to a financial services entity (e.g., personal address and contact information).
- **Balance data:** Information pertaining to the amount of money in a deposit-based account held by the customer at any given time (e.g., e-wallet account balance).
- **Transaction data:** Information that is generated through transaction activity on a customer's account (e.g., withdrawals, transfers, and deposits).

In conjunction with customer data and balance data, transaction data facilitates the bulk of open banking use cases.

- **Identity verification results:** Confirmation of a customer's identity through a validation process using personal and financial information (e.g., KYC verification results). In Canada, there are other digital identity solutions currently in development (e.g., Verified.me).
- **Aggregated data:** The compilation of information across multiple customers that may be de-identified and/or summarized (e.g., average account balances across an age band or postal code). This would enable a variety of new use cases (e.g., "people-like-me" comparisons), but would require significant additional effort from data generators.

From a data-sharing perspective, customer-generated data, balance data, and transaction data would fall under customer data.

The inclusion of public data, identity verification, and aggregated data would promote competition in the market, but the additional complexity and potential liabilities involved in sharing them, while also protecting competitive insights that could be extracted from that data, should be carefully considered.

It is also important to note that the open banking frameworks in other jurisdictions allow institutions to enter private commercial agreements to make data excluded from the scope of open banking policies available to third parties.

How far back should data be made available?

Choices made by other jurisdictions:

No specific historical data requirments

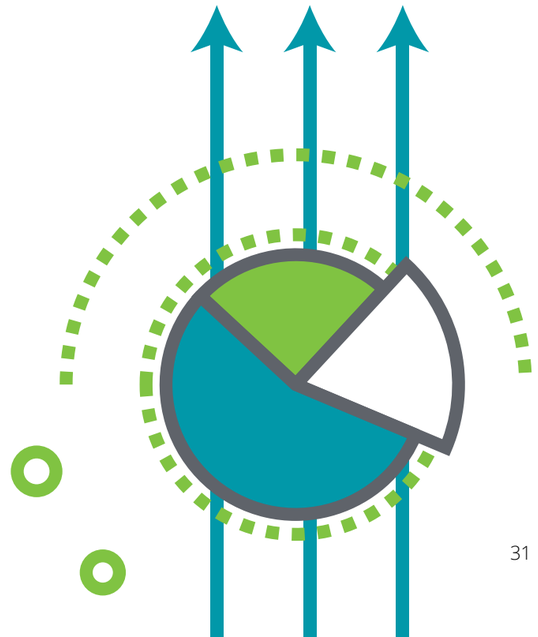
Rolling historical data requirements

Initiation date requirement

** Note: Varies by data type*

Different jurisdictions have taken different approaches to historical data requirements imposed on data generators. One approach is to mandate an "initiation date" (i.e., the date from which data must be made available upon the public launch of the open banking framework), while another is imposing a "rolling requirement" (i.e., the amount of historical data (in months/years) that should be provided from the date of a data request). Some jurisdictions, like the UK, have also made different decisions based on the type of data (e.g., aggregated data are shared on a 25-month rolling basis, while transaction data have an initiation-date requirement).

When establishing its own rules surrounding this issue, Canada must recognize the tradeoff between the value delivered to Canadians and the burden imposed on data generators. For instance, while longer-term historical data may offer invaluable trends-based spending and savings advice for consumers, many institutions may have a limited amount of data available in their existing digital datasets.



Who should be required to open access to their data?

Choices made by other jurisdictions:

The requirement to open access to data can be institution based (i.e., all financial institutions with a certain classification, such as Schedule I and Schedule II banks), or activity based (i.e., all financial institutions that provide Canadians with the functions discussed on page 27).

An activity-based approach would ensure the framework is flexible enough to adapt to new types of non-traditional institutions that may emerge over time, and may foster a more level playing field where all players offering competing products and services are required to make data available regardless of their legal classification. However, it creates a more nebulous governance environment, as lines between institutions in scope and out of scope blur (e.g., Would PayPal's online wallet be considered a "deposit account"?). Furthermore, the current financial regulatory systems in Canada are institution-based, meaning activity-based requirements would necessitate either a change in a current regulatory body's scope or a new regulatory body.

It is also important to consider whether an open banking framework would act as a stand-alone framework within financial services or exist as part of a broader open data framework across industries. In the case of the latter, the concept of data reciprocity could be used to enable other organizations to participate in the open data system.

Australia is actively exploring the concept of reciprocity, whereby data recipients who hold "equivalent data" to the financial data being shared with them by data holders (this term has yet to be fully defined by Australia's Competition and Consumer Commission) would be required to share these data with data holders at the request of a consumer. It is important to note that reciprocity is being explored for the purposes of improving data accessibility (as opposed to strictly increasing data access) and is based on the principle of explicit consumer consent. Under a proposed reciprocity framework, data holders would not be allowed to request data from data recipients unilaterally; they could only do so in situations where consumers have requested data recipients to share their "equivalent data."

Creating an open banking framework for Canada | An open banking framework for Canada

How should the rollout work?

Choices made by other jurisdictions:

Beyond account coverages, different jurisdictions have also rolled out open banking regulations in different ways. To determine what will work best in Canada, stakeholders must ask two key questions:

1. How much time will data generators need to comply with the technical standards behind open banking?

Regulators must strike the right balance between launching open banking in a timely fashion and making sure institutions have enough time to comply, so as to avoid jeopardizing the safety of user data.

Regulators must also be aware that, in markets where some form of open banking has already been deployed, uneven and/or non-customer-friendly compliance risks expose the customer to less-than-optimal solutions, which may turn away the very customers that would otherwise be enthusiastic first adopters.

2. When the proverbial switch is flipped on, should there be different timelines for different entities?

It should be noted that several jurisdictions (such as the UK and Australia) have made the conscious decision to impose open banking on large, incumbent banks before other types of financial institutions, essentially "staging" the deployment of open banking. This is partially to allow the framework to evolve safely—without exposing the financial services ecosystem to undue risk presented by smaller financial institutions with limited IT resources—and partially to allow the punitive intent behind open banking to play out. In these cases, open banking was introduced, in part, to increase competition against large, incumbent banks. Australia has also made the conscious decision to stage the deployment of open banking by product type, with data on basic transaction accounts being made available first, followed by more complex products (e.g., mortgages). The EU, on the other hand, did not have this original mandate and, as a result, opted to open open banking to all accredited parties simultaneously.

Canada will need to carefully weigh the merits of both options, as well as the reasons behind open banking deployment, before coming to a decision.

Which types of data recipients will be allowed?

Choices made by other jurisdictions:

None

Data consumers only

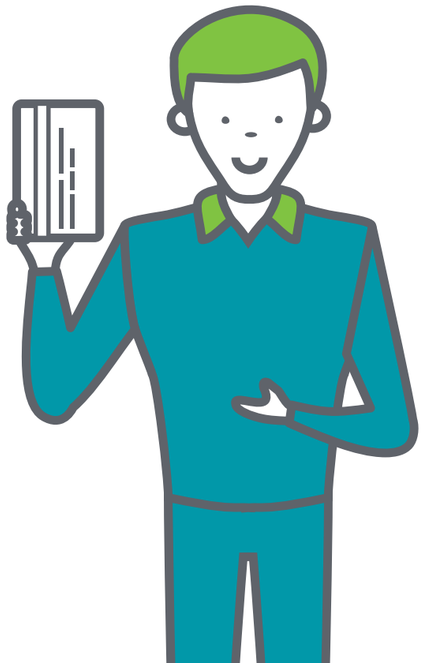
Data consumers and data transporters

One thing that seems to be consistent across all jurisdictions is that only entities that meet their central governing body's risk-based, tiered accreditation criteria are granted access to customer data (details on accreditation criteria are outlined on page 51).

In addition, there are only two types of data recipients: data consumers and data transporters. Data consumers are end users of customers' financial data (e.g., fintechs and other third-party providers) while data transporters are intermediaries that facilitate the flow of data-to-data consumers. The key difference between the two is that the latter does not create value from the storage of data.

While data consumers are a prerequisite for open banking, data transporters are not necessarily required. This is because they tend to introduce significant risk to the ecosystem by acting as a central source of large volumes of data, making it possible for a single breach to threaten countless data generators and customers. However, these players also provide value to the ecosystem by creating interoperability between financial institutions, as well as across geographies where differing open banking systems have already been implemented. In most jurisdictions, there is no regulatory distinction between data consumers and data transporters. Transporters are thus required to be accredited based on the same criteria as consumers (e.g., in the UK, data transporters must be accredited AISPs).

Ultimately, the value of data transporters is dependent on the level of standardization of the data transfer mechanisms employed by the various data generators in scope. This is explored in greater detail on page 39.



Creating an open banking framework for Canada | An open banking framework for Canada

Canadian market factor: Governance of non-traditional payment service providers (PSPs)

Existing payments regulation in Canada is heavily focused on governing systemically important and prominent national payment systems, such as LVTS and ACSS, leaving non-traditional PSPs relatively free of regulatory oversight.

The Retail Payments Oversight Framework (RPOF) is an effort to ensure non-traditional PSPs are governed effectively, thereby preserving the safety and soundness of the Canadian payments ecosystem, fostering efficiency and innovation within payments, and protecting end-user interests.

Open banking's accreditation process is likely to involve many of these same players, so it is important that the RPOF and open banking regime are coordinated. This would help prevent the creation of conflicting and overlapping legislation and optimize the allocation of resources and responsibilities across regulatory bodies.

What access rights should data recipients have?

Choices made by other jurisdictions:

Another thing Canadians will have to consider when building their open banking framework is how data recipients will ultimately access customers' data. Based on existing open banking systems, there are essentially two ways to access data:

- **Read access,** which allows data recipients to obtain copies of customers' financial data and use it for such activities as data aggregation; or
- **Write access,** which allows data recipients to make modifications to customers' financial data held by other institutions.

Write access would allow data recipients to act on behalf of the customer in areas such as payment initiation, account opening/closing, and changes to information (e.g., change of address). While this would obviously present many opportunities for financial institutions, it would also introduce new complexities—particularly in the realm of security.

Because data recipients would be able to make changes to customers' accounts and move money on their behalf, institutions would have to take tremendous steps to mitigate the risk of a data breach. Data generators would have to build complex systems to ensure customers' information was safe—a process that would require significant time to implement.

The Retail Payments Oversight Framework and payment modernization initiatives have already taken some steps in addressing the challenges related to write access. To avoid duplication of efforts or contradictory guidance, the scope of An open banking framework should take these initiatives into account.

Canadian market factor: Canadian payments modernization

As the industry contemplates open banking, Payments Canada is also taking steps to reshape Canada's banking sector through the modernization of Canada's two primary payments systems, the Large-Value Transfer System (LVTS) and the Automated Clearing Settlement System (ACSS). LVTS will be replaced by Lynx, a high-value payments system that will process payments in real-time with settlement finality. ACSS will be replaced by the Real-Time Rail (RTR) system and the Settlement Optimization Engine (SOE) system.

RTR will facilitate the transfer of low-value funds in real time and will further support the development of overlay services (i.e., value-adding services owned by third parties and deployed on RTR infrastructure), ultimately spurring payment innovations. SOE will enhance the clearing of less time-sensitive batch paper and electronic payments, enabling faster and more convenient payments for businesses in Canada. Through this modernization effort—as well as the Retail Payments Oversight Framework (detailed on page 35)—third-party payment initiation will likely be addressed outside of an open banking framework.

Another key element of the modernization effort is the adoption of the ISO 20022 standard, which will enrich the data transmitted with payments. In designing open banking, the interplay between its scope and additional data gathered through ISO standard will need to be carefully examined.

In addition, as Canada prepares for the introduction of RTR, it would be prudent to consider how the risks associated with screen scraping practices are mitigated in advance to reduce vulnerabilities for fraud (e.g., credential sharing).

2. Standards

The choices made by other jurisdictions around the level of standardization help define how prescriptive and centralized technical standards (if any) will be, and how overall system oversight will be structured.

While building an open banking framework, Canada should answer these questions:

- How should data sharing standards be developed?
- How should consent and authentication be managed?
- How should system oversight be structured?
- Who should participate in oversight?

How should data-sharing standards be developed?

Choices made by other jurisdictions:

The approach to data-sharing standardization represents a delicate balance between promoting competition among new entrants and existing players, and ensuring overall financial system security as well as operational integrity.

Here, regulators have two main choices:

1. **Centrally defined standards:** Regulators can develop highly prescriptive technical standards that mandate specific technologies and processes for data sharing, while strictly enforcing compliance;

2. **Generator-led standards:** Regulators can define broad, high-level data-sharing policies, while allowing financial institutions and third parties to independently develop standards, technologies, and processes to abide by them.

While developing prescriptive data-sharing standards would promote greater system security, increase interoperability among players, and drive down development and integration costs, strict standards could put undue compliance burden on some players (both financial institutions and third parties alike) who may not have the resources to develop against them.

Furthermore, they could hinder the ecosystem's ability to quickly adopt new and more effective data-sharing technologies, as this would require significant re-writing of standards documents.

On the other hand, developing broad data-sharing policies (e.g., a code of conduct) while leaving the creation of standards, technologies, and processes to industry players would allow for greater overall flexibility and responsiveness to change, and may quicken the pace of open banking adoption. Furthermore, it ensures that the data-sharing approach is informed by deep industry expertise. However, this could lead to the emergence of multiple competing standards that compromise interoperability and system security, as well as increase development and integration costs for all players (who may have to develop multiple data-sharing processes to integrate with different partners).

In order to balance the promotion of competition and innovation with system security and integrity, the Canadian open banking movement should consider a hybrid approach. This would mean developing certain centrally mandated minimum data-sharing criteria (to ensure baseline interoperability and protect customer data), but leaving the majority of design choices to the discretion of individual players and/or industry consortia.

How should consent and authentication be managed?

Authentication

Choices made by other jurisdictions:

Consent

Choices made by other jurisdictions:

A successful model for data sharing should include secure and user-friendly processes for both customer authentication and consent.

When it comes to managing customer authentication, there are essentially two options: place the responsibility in the hands of the data generator or the data consumer. Managing authentication through the data consumer may lead to a smoother user experience, since login would be completely integrated into third parties' interfaces and match their user experience design. That said, it may also expose customers to additional risk, since their banking credentials would be shared with each third party they choose to use. Furthermore, requiring data recipients to develop secure authentication processes could act as a barrier to entry for smaller third parties, as such an endeavour will inevitably be a complex and time-consuming process.

If authentication is assumed to be conducted by the data generator, there are three possible models:

- **Embedded:** At the time of authentication, the customer enters their banking credentials into a "widget" hosted and operated by the data generator that is embedded directly into a third-party interface;
- **Redirect-based:** At the time of authentication on a third-party platform, the customer is redirected to their data generator's website (i.e., online banking portal) where they enter their credentials and, after authentication, are redirected back to the data recipient; or
- **Decoupled:** At the time of authentication, the customer is asked to navigate to the data generator's online portal. After authenticating, the customer retrieves and manually copies and pastes the code into the third-party website.

Each of these methods offers its own balance between user experience and security. While the embedded workflow is convenient for customers, it increases the risk of phishing. The redirect-based flow is the most common among internet services (e.g., Facebook) and customers are largely familiar with the process. The decoupled flow is less commonly used, as it requires manual effort from customers that creates additional friction and may hinder the pace of adoption. However, it is less susceptible to phishing attacks than the other two models.

Phishing

Phishing is a type of socially engineered fraud where bad actors attempt to obtain sensitive information for malicious purposes using deceptive means. For example, a bad actor may set up a fake third-party website that redirects a customer to a page disguised as their banks' interface, stealing their credentials, other personal information and, ultimately, their money.

The elements of authentication

Authentication can rely on a combination of evidence:

- Knowledge (e.g., password)
- Possession (e.g., key, mobile phone)
- Inherence (e.g., fingerprint)

Requiring more than one form of evidence is known as "multi-factor authentication" and increases the safety of the authentication flow at the cost of user experience (e.g., by requiring them to receive a code on their mobile device and input it into the system). Precedents set by other jurisdictions suggest that requiring more than one form of evidence is prudent.

Canadian market factor: Role of a digital ID utility

Digital ID is the electronic storage of identity information that allows people to identify themselves online without having to continuously present physical documentation. If a standard form of digital ID is developed and mandated in Canada, authentication would not need to happen entirely on the bank's online interface. The utility providing the digital ID service could serve as the central authentication manager, leading to greater safety and security, improved user experience, and reduced authentication costs for market participants.

In considering the evolutionary path for open banking, it would be important to consider how digital ID might help banks and other data generators better manage authentication risks, enable more thorough fraud analytics, and create a more harmonized customer experience.

Under open banking, customers will control their own data and should be able to provide specific direction regarding the transfer and use of that data. The consent on how this data is used could occur on the data generators' side, data recipients' side, or both.

Regardless of which model of consent is chosen, its ultimate purpose should be to enforce transparency and ensure customer consent is meaningful and informed. A robust customer consent process should also go beyond the requirements outlined in PIPEDA—particularly in the areas of explicitness and enforcement—as these standards tend to be underdeveloped, due to the legislation's age.

To achieve these end goals, the Canadian open banking movement should consider borrowing a few common best practices from other jurisdictions. For one, consent prompts should be simple—ideally written in plain language and concisely displaying all important information on one screen. This ensures that the authentication and consent process is not a barrier to open banking adoption.

Additionally, customers should be able to withdraw consent at any time. In line with the shift of data control back into customers' hands, they should be able to revoke access if desired. However, the original data held by the data generator should not fall under this principle, as is often required by existing regulatory frameworks for AML purposes.

Canadian market factor: Updates to PIPEDA

Open banking will hinge on privacy law reform. While current privacy laws dictate how information is kept, stored, and used, open banking will have to expand on these regulations—focusing specifically on how data will be shared between financial institutions and third-party providers.

Canada is in the midst of a consultation process for changes to PIPEDA, which would bring it into line with much of the changes brought by the European Union's General Data Protection Regulation (GDPR). GDPR mandates financial institutions to erase customer data (collected directly from customers and received from third parties) upon customer request if one of the following six conditions is met:

1. The personal data is no longer necessary in relation to the purposes for which they were collected or otherwise processed

2. The data subject withdraws consent [...]

3. The data subject objects to the processing [...] and there are no overriding legitimate grounds for the processing [...]

4. The personal data have been unlawfully processed

5. The personal data have to be erased for compliance with a legal obligation [...]

6. The personal data have been collected in relation to the offer of information society services [...]

GDPR encompasses both digital and physical documentation and includes backup files. However, the right to be forgotten may be overruled, or delayed, for some or all data classes due to regulatory obligations imposed on the controller of that data (e.g., record-keeping for accounting and taxation).

As open banking is developed in Canada, care must be taken to ensure that open banking abides by any changes to PIPEDA and does not possess any glaring gaps in coverage with respect to the consensual sharing of financial services data between open banking and PIPEDA.

In other jurisdictions like Australia, specific privacy provisions are included in the open banking policies to augment existing privacy laws in areas like granular consent and the rights to be forgotten.

Creating an open banking framework for Canada | An open banking framework for Canada

How should system oversight be structured?

Choices made by other jurisdictions:

An open banking system will require two phases of governance: the first will be needed to define the overall system, while the second will provide ongoing operational oversight (e.g., acting as a dispute resolution body for liability issues between data generators, data recipients, and customers).

The responsibilities of each governance structure will be unique. Below are a few examples of what they may entail:

Phase 1:
Defining the open banking system

- Develop the data-sharing standards that data generators must abide by to make customer data available;
- Develop the specific accreditation criteria that governs which data recipients are allowed to request data from data generators; and
- Define the liability framework that clearly outlines the roles and responsibilities of data generators, data recipients, and customers.

Phase 2:
Operating the open banking system

- Provide ongoing oversight over data generators and accredited data recipients (e.g., regularly auditing data recipients to ensure accreditation criteria are being met);
- Act as a central dispute resolution body for customer complaints and liability issues;
- Support the development and execution of customer education;
- Require a mandatory insurance product, similar to the CDIC, that pays out in case of disruptive losses that lead to the complete failure of a data recipient (this program could be funded by a mandatory fee as part of the accreditation process);
- Create a digital identity, consent, and authentication management system; and
- Manage the recovery of variable costs incurred by data generators to make data available to third parties.

The responsibilities of governance and oversight of the open banking system can be either:

- Centralized into a consolidated governance function; or
- Distributed to data generators, data recipients, and industry bodies that represent customers to self-regulate through voluntary industry "codes of conduct"; or
- Divided between these two approaches, whereby some pieces of governance are mandated by a centralized authority, while others are distributed to industry participants to develop "codes of conduct."

While the ideal allocation of responsibilities between these various parties is up for debate, Canadian stakeholders would be well served to keep the aforementioned guiding principles in mind as they determine the distribution best suited to a Canadian open banking framework.

Some of the ways these guiding principles can be used to streamline the decision-making process include:

Value

Prevent conflicts of interest that inhibit the delivery of value to Canadians. To ensure the open banking system delivers true value to Canadians, the interests of the customer must be represented across governance functions. Understanding this, measures should be put in place to ensure neither data generators nor data recipients have sole control over the development of an accreditation framework, as this could lead to an overly complex process (that unduly limits participation from data recipients) or an overly open ecosystem (that exposes the financial services ecosystem to undue risks).

Safety

Leverage regulatory authority where needed to protect the safety and soundness of the financial system in Canada. The governance framework should ensure that Canadians are not exposed to undue risk. For example, the system should consider whether access to datasets through non-Open Banking methods (e.g., screen scraping) should be permitted for data that could be made available through open banking. Ideally, the open banking framework should provide more secure, cost-efficient, reliable, and customer-friendly access to data, potentially making alternatives (such as screen scraping) an unnecessary risk to the system.

Transparency

Ensure that Canadians are given full clarity and transparency when sharing data. In order to ensure that Canadians have consistent transparency when sharing data, standards around what information is being shared and how it will be used should be put in place. These standards may lead to a common screen for information sharing, as is being established in other jurisdictions.

Adoption

Efficiently leverage the various participants in the ecosystem to minimize the duplication of effort. Given the variety of concurrent efforts regarding the oversight of financial institutions and system infrastructure (e.g., RPOF), the governance framework should be designed to minimize the duplication of responsibility between parties. Economies of scale could be realized by centralizing governance responsibilities, but should be considered on a case-by-case basis to decrease the total cost of the system. For example, managing liability issues or cost recovery through a single central entity may help simplify these processes (at a lower cost) for all participants in the open banking system.

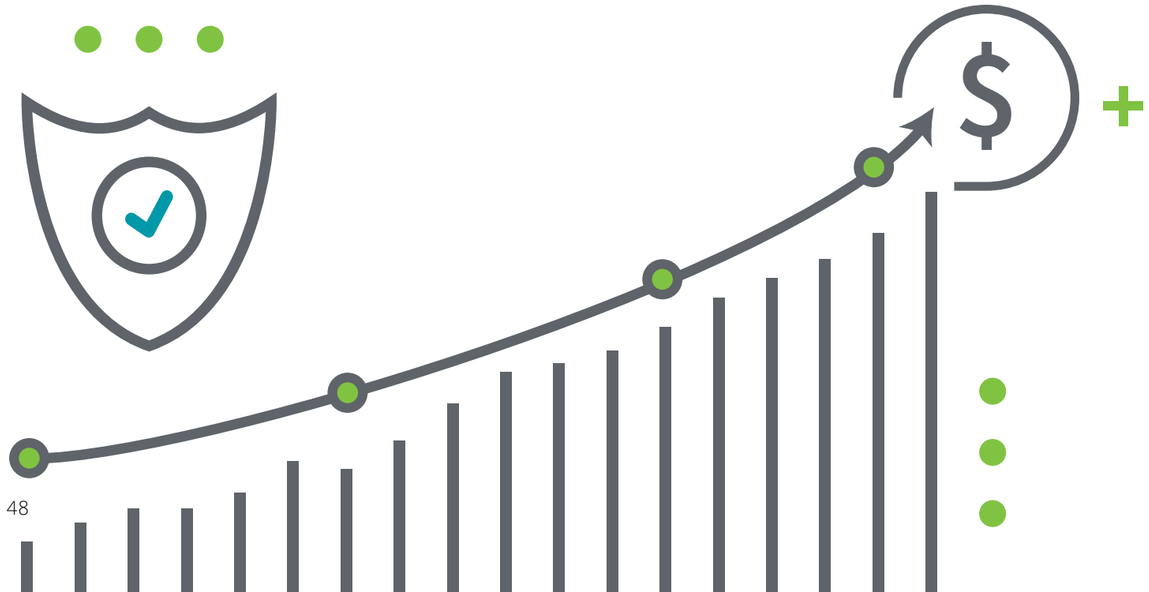
Who should participate in oversight?

Typically, even centralized oversight bodies are comprised of both regulators and market participants. For instance, in the UK, the Open Banking Implementation Entity, while created by the Competition and Markets Authority (a regulator), is funded by the UK's nine largest banks. In the EU, while regulators are responsible for accreditation of third parties and are responsible for policy development, bringing principles-based policy into implementation across Member States requires the assistance of various standard-setting organizations and consortia (e.g., the Berlin Group).

This report is designed to offer considerations for open banking in Canada, regardless of which model of governance and oversight is selected, and who is ultimately involved in this process. That being said, the possible outcomes differ based on the choices made here.

For example, under a highly centralized governance model, the scope of data generators would likely depend on who participates in the governance entity. For instance, a regulator-led central entity would likely have the authority to mandate that a broad set of participants—for instance, credit unions and trusts—be included as data generators. A consortium-led or industry-led effort, on the other hand, would rely on voluntary participation from financial institutions, likely making the scope of data generators more limited.

Ultimately, as open banking in Canada is explored further, the role and structure of the central body will play a key role in its development. Because of this, it is a choice that should be made early in the process.



3. Commercial and liability model

The choices made by other jurisdictions around the commercial and liability model in place define how costs and liabilities will be distributed among market participants.

While building an open banking framework, Canada should answer these questions:

- How do data recipients gain access to generators' data?
- How should liability be managed?
- What is the supporting economic model?
- How often should data requests be allowed?

How do data recipients gain access to generators' data?

Choices made by other jurisdictions:

There are two models that could be used to facilitate access to generators' data:

1. **Commonly agreed-upon accreditation requirements and standard contracts between data generators and data recipients.** In this model, data recipients would have to receive certification to demonstrate their compliance with pre-set criteria (e.g., regarding data privacy and security). Certain elements that concern the data generators' and data recipients' relationship (e.g., method and terms of cost recovery, liability) would be defined by a standardized contract with some flexibility to accommodate the unique circumstances of the data-sharing arrangement.

2. **Bilateral commercial agreements (between data generators and data recipients)**. In this model, both access to the ecosystem and specific elements would be defined through one-to-one agreements between data generators and data recipients, where parties have complete flexibility to negotiate the terms of the agreement.

Commercial agreements would more rapidly adapt to changing conditions, but may limit the efficiency of the system (e.g., financial data aggregators would be required to negotiate individual bilateral contracts with every financial institution participating in open banking as a data generator).

A commonly agreed-upon accreditation framework would simplify the process of gaining access to data, ultimately allowing more third parties to participate in the open banking ecosystem. However, it would be less flexible to changes in marketplace dynamics, and would require continuous updating to accurately reflect the broader environment in Canada.

If a central-accreditation-based system is selected, Canada may look to other jurisdictions to inspire the development of:

- **Security and privacy protocols:** To responsibly manage sensitive personal and financial data, and make sure that data recipients are not introducing undue security risks into the system.
- **Indemnity insurance:** To provide data generators with some reasonable certainty that data recipients will be able to pay out if a liability issue occurs.
- **A defined customer complaint management process**: To provide customers with some reasonable certainty that accredited third parties will be able to support them in case of any issue.
- **Mitigation measures for material disruptions:** To ensure appropriate protocols are in place in the event of system failures, security breaches, and other blockages to continuity.

The intended "use case" of data is a hotly debated topic in other jurisdictions with more advanced open banking systems. Including use case as a criteria would be helpful in protecting consumers from malicious actors; however, it may limit the scope of third-party providers with novel business models, potentially limiting innovation in the marketplace.

How should liability be managed?

Choices made by other jurisdictions:

Generally, open banking should decrease total risk in the system by reducing the need for customers to share their banking credentials with screen scrapers. However, it may result in a shift of liability from customers (who are in breach of their contract with banks by screen scraping) to other participants in the system. As a result, a clearly defined liability framework is critical to garner buy-in from data generators and data recipients alike.

This type of liability framework, however, is highly contingent on a variety of other framework choices. Below are some of the choices observed in other jurisdictions:

- Based on previous cases of open banking adoption, it is helpful if a liability framework is compatible with other existing regulations, rather than superseding them. This prevents the development of overlapping/conflicting requirements and ensures all participants have a common understanding of the roles and responsibilities of each player.
- For unintentional data breaches, many jurisdictions have chosen to assign liability to the party responsible for the breach itself (the data recipient in the vast majority of cases). In this type of scenario, the data recipient typically has adequate liability coverage for data breaches, and any accreditation program for data recipients includes both a security standard and a liability coverage standard. This framework has been found to raise customer trust in open banking, even after a hypothetical data breach incident occurs.
- In cases where companies intentionally misuse customer data, such as when malicious actors acquire accreditation, some jurisdictions have assigned liability to the body that granted that accreditation and/or extended the accreditation most recently.
- Many jurisdictions currently allow data generators to sever a linkage with a data recipient if they suspect either an unintentional data breach or misuse. These data generators are responsible for reporting suspected breaches/misuse within a short time period to other data generators and/or the accreditation body to minimize the impact of the breach.
- Many open banking jurisdictions believe participants should be responsible for their own actions, but not the actions of others (e.g., data generators should not be liable for losses caused by data recipients). So, while account providers are the designated first responder in case of a loss, many jurisdictions have controls in place that allow them to seek recourse from the third parties responsible. This ensures account providers are not left unfairly holding the burden of liability, leading to greater participation from account providers in open banking. Certain jurisdictions also mandate capital requirements and/or indemnity insurance to third-party providers to provide some protection to account providers.
- In many jurisdictions, data generators have an obligation to report all in-scope information to data recipients truthfully, but they are not held liable for unintentional mistakes/inaccuracies in transferred data.

What is the supporting economic model?

Choices made by other jurisdictions:

To make data available, data generators are likely to incur both upfront fixed costs as well as ongoing variable costs. An open banking framework must outline whether data generators are allowed to recover their variable costs, for example, through a minimal fee charged to data recipients. When contemplating whether this is the right option for a Canadian open banking framework, stakeholders must consider a number of different factors:

- **Fairness to data generators:** Beyond the direct costs of making data available, data generators are likely to face additional indirect expenses (e.g., customer complaint management). Regulations should ensure they are able to sustainably perform these functions without being unfairly burdened by the process.
- **Comparison to current state for data recipients:** API-based solutions are likely to be significantly less resource-intensive (and thus, less costly) than the solutions that data recipients use today. As a result, data recipients' costs of accessing customers' financial data is likely to be lower than the current state.
- **Barrier to entry:** Charging fees for access to data may act as a barrier to the market. This could cause negative consequences (such as the stifling of innovation) or positive results (such as the stifling of low-value use cases), depending on the size of the data transfer fee.

How often should data requests be allowed?

Choices made by other jurisdictions:

** Note: No information is available about data request limits in Japan*

In the UK, data recipients are limited to making four requests in a 24-hour period, unless a higher frequency is agreed upon by the data generator and data recipient. However, customers can initiate data requests an unlimited number of times, which is similar to the level of access currently provisioned through online banking services, for example, in instances where customers have 24/7 access to their banking information through their bank's online interface. This distinction between data requests initiated by recipients (which are often limited) and by customers (which are often unlimited) is common across many jurisdictions.

Allowing for a large number of requests enables additional use cases (e.g., an account balance monitor that notifies users when they are approaching overdraft) at the cost of a greater burden to data generators (i.e., of data transfer). Depending on whether a fee is charged to data recipients for every request they make, a limit may or may not be necessary to prevent data generators from being overwhelmed by a large volume of requests.

Conclusion

Canada sits at an inflection point in the modernization of its financial services ecosystem. When looked at in conjunction with payments modernization and an expected overhaul of privacy legislation via PIPEDA, open banking represents the third pillar of a new landscape, one that will reshape customer expectations for the delivery and consumption of financial services.

If all goes according to plan, the financial services industry, and financial customers of the future, will all benefit from lower barriers to customer movement between organizations; more personalized and tailored financial experiences; and the automation of traditionally time-consuming procedures and tasks.

This movement, however, will not overhaul the financial services ecosystem overnight. Rather, the major changes arising from open banking will likely arrive gradually, meaning, a significant window of opportunity exists for both new entrants and existing players alike. During this time, longstanding institutions would be well served to address pain points in their current banking solutions if they hope to play a leading role in reshaping the market.

Open banking is just one step in a broader movement of returning control over customer data back where it belongs—the end customer. Customers' right to data control is about far more than just financial data, which means open banking stands to pave the way for other industries as well. By taking the first step in a deliberate and calculated manner, open banking can act as a template for others, illustrating the leadership role that financial services has in Canadian society and in protecting the customer above all.

Endnotes:

[1] ZDNet, "Westpac predicts Open Banking to cost AU$200m to implement," by Asha McLean, October 12, 2018, https://www.zdnet.com/article/westpac-predicts-open-banking-to-cost-au200m-to-implement/ accessed on March 18, 2019.

[2] Competition & Markets Authority, "Making banks work harder for you," August 9, 2016, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/544942/overview-of-the-banking-retail-market.pdf accessed March 18, 2019.

[3] Australian Government, "Review into Open Banking in Australia," 2017, https://static.treasury.gov.au/uploads/sites/1/2017/08/Review-into-Open-Banking-IP.docx accessed March 18, 2019.

[4] The Government of Japan, "Drive Innovation and Trade," https://www.japan.go.jp/abenomics/innovation/index.html, accessed March 18, 2019.

[5] Abacus Data, prepared for Canadian Bankers Association, "How Canadians Bank," 2016, https://www.cba.ca/Assets/CBA/Documents/Files/Article%20Category/PDF/info-howCanadiansBank-poll-2016-en.pdf, accessed March 18, 2019.

Contacts

Rob Galaski
Global Managing Partner
Banking & Capital Markets
rgalaski@deloitte.ca

Todd Roberts
Partner
Canadian Payments Leader
toddroberts@deloitte.ca

Hwan Kim
Canadian Open Banking Leader
hwankim@deloitte.ca

www.deloitte.ca

Designed and produced by the Deloitte Design Studio, Canada. 18-5879T