FINAL REPORT

DATA-SHARING FRAMEWORKS IN FINANCIAL SERVICES:

Discussing Open Banking Regulation for Canada

Author

Markos Zachariadis
Alliance Manchester Business School,
University of Manchester

GRI | GLOBAL RISK INSTITUTE

AUGUST 2020

ABOUT THIS REPORT:

At its core the financial services industry is predominantly an information business. This is mainly because data is increasingly becoming the key ingredient and the basis for many of the products and services offered in finance. It is often seen as a fundamental "asset" to stimulate competition and boost growth in the sector. From consumer and business banking, to payments, trading, wealth management, investment banking and insurance, data is being used not only to maintain financial ledgers and facilitate effective communication of trade and payment instructions, but to also assess risk, manage finances, forecast market movements, and optimize portfolio management. As a result, access to and the sharing of data can provide significant advantages to players in the industry and change the shape of competition in financial services.

Data-sharing frameworks in financial services: Discussing open banking regulation for Canada

Report for the Global Risk Institute (GRI)
Toronto, Canada

August 2020

Professor Markos Zachariadis
Greensill Chair in Financial Technology (FinTech) & Full Professor in Information Systems, ***Alliance Manchester Business School****, University of Manchester* | Member of the Global Future Council in Financial & Monetary Systems, ***World Economic Forum*** | FinTech Research Fellow at the *Cambridge Digital Innovation Centre*, ***University of Cambridge***

Introduction to data-sharing and open data in finance

At its core the financial services industry is predominantly an information business. This is mainly because *data* is increasingly becoming the key ingredient and the basis for many of the products and services offered in finance. It is often seen as a fundamental "asset" to stimulate competition and boost growth in the sector. From consumer and business banking, to payments, trading, wealth management, investment banking and insurance, data is being used not only to maintain financial ledgers and facilitate effective communication of trade and payment instructions, but to also assess risk, manage finances, forecast market movements, and optimize portfolio management. As a result, access to and the sharing of data can provide significant advantages to players in the industry and change the shape of competition in financial services.

This realization – around the significance of access to data and information – led many institutions in the various sub-sectors of the finance industry to invest heavily in Information and Communication Technologies (ICTs) with the hope that they would gain a competitive edge through utilizing data for better money management, cost-effective operations, new product development, and customer acquisition. However, this wasn't always the main focus. Traditionally, investments in financial technologies have been seen as ways to increase operational efficiencies and cut costs. For example, during the 1950s and into the 80s, banks sought to deploy mainframe computers to mechanise record keeping and facilitate more efficiently a multitude of transactions (Bátiz-Lazo et al., 2011). About the same time globalization gained momentum and international trade flourished leading to the emergence of financial telecommunication infrastructures and the creation of messaging standards that allowed corresponding banks to automate data processing (i.e. STP), reduce manual interventions, and speed up their operations (Scott and Zachariadis, 2012; 2014). In the 1990s, as technology was becoming cheaper and personal computers were deemed more accessible, banks increasingly digitized their processes aiming to minimize paper-based tasks. The penetration of the internet also allowed for the development of digital networks and the creation of new communication channels internally and with customers.

While the above efforts were necessary steps in order to achieve better results and provide the pillars for the future financial services, the recent "FinTech[1] revolution" has forced conventional players to re-consider their technology (or digital) strategy and focus more on re-designing processes, re-thinking value creation, and monetising data assets. It's a bit ironic to think that these investments in information technologies (IT) – now called "legacy" infrastructures and old-generation IT – are considered a barrier to digital transformation and

[1] While FinTech as a word is an abbreviation of "financial technology", it is most often used to refer to the emergence of an ecosystem of technology startups that innovate at the heart or on the fringes of financial services and provide solutions that can benefit consumers and financial institutions to better handle money and their finances. As explained above, the key difference between "traditional" financial technologies and "new" ways of introducing technology in finance is that older technology implementations focused more on creating more cost-effective operations and achieving efficiencies through automation, while, new FinTech is geared more towards re-considering entire business processes and introducing new business models in finance. Popular commentators in this space, such as Chris Skinner, have described FinTech as the "R&D function of financial services in the digital world" (see full blog here: https://thefinanser.com/2015/01/ghgh.html/). Another key characteristic of the recent FinTech wave has been the interest entrepreneurs and investors-outside of financial services, and mostly from the tech world, have shown in the finance industry in order to take advantage of existing inefficiencies and 'disrupt' the *status quo*.

one of the reasons incumbent financial institutions find it difficult to adapt to the new technological regime in finance – especially when it comes to the implementation of modern data access technologies.

In the context of this new wave of "digitalization"[2], the finance industry has witnessed an increase of data-sharing within and across financial institutions aiming to accommodate solutions that demand a combination of data points residing at different systems. Data-sharing in finance can be traced back to the use of interorganizational financial systems and electronic data interchange (EDI) networks[3] which enabled bilateral data feeds. More recent technologies such as *screen-scraping* and *application programming interfaces* (APIs) are being used systematically by financial institutions and FinTechs to enhance data-sharing opportunities and explore new possibilities in service development.

The emergence of APIs in banking

An application programming interface (API) is a technology or, otherwise put, a set of instructions that allows two systems or computers to "talk" to each other over a network (most usually the web or the internet) using a common data standard. APIs published by a provider are usually accompanied by documentation that specifies their functionality, business use, uptime, constraints, legal implications, etc. For that reason, they can also be understood as a contract to engage in a particular relationship or consume a service[4]. APIs have gained significant momentum over the last couple of decades in the technology sector but also in many more industries, and have become the de facto standard for sharing data and enabling communication between colleagues, partners, or third-parties. This is largely because they are scalable, secure, and standardized. For that reason, they can be reused in different settings with very little cost of development (Jacobson et al., 2012). Initially, the use of APIs in banking was limited to private APIs that were exclusively available to internal staff and 'clients' within the boundaries of financial institutions. Such 'closed' APIs are often used to unlock the data resources of the organization and attempt to break data silos utilizing data in new applications and systems while helping the business run better.

Having said that, APIs are not restricted to internal or closed. They can also be conceptualized as "boundary resources" that establish simplified and standardized connections beyond the organization and with selected partners or groups of authorized third-parties (Ghazawneh and Henfridsson, 2013). This approach offers the possibility for open innovation and the development of an ecosystem of third-party providers (TPPs) who can design and deliver new products. In payments, such 'open' or 'external' APIs, have been used by card networks like VISA and MasterCard to integrate their infrastructure with

[2] The difference between 'digitization' and 'digitalization' is that the former focuses more on the effort to digitize existing processes and tasks (i.e. the move from analog to digital or from a paper-based system to a digital representation of the same data or tasks), while the later signifies predominately "a sociotechnical process" and move to a digitally-native way of engaging in economic activity that suggests new ways of creating revenue and the adoption of novel business models (Tilson et al., 2010). Digitalization often implies a more customer-oriented inclination to problem-solving and engaging with people to address particular needs.

[3] EDI systems, which flourished during the 1980s and 1990s, allowed trading partners to exchange structured financial information electronically between separate computer applications (Bátiz-Lazo and Wood, 2002; Iacovou et al., 1995). These were mostly proprietary and less standardized which meant partners would need to make an investment in order to establish such relationships.

[4] For a detailed discussion on the various approaches and definitions to APIs as well as their use in open banking see section "Deconstructing APIs" in Zachariadis and Ozcan (2017).

selected e-commerce partners (e.g. VISA Checkout) providing a better customer experience online, or to offer more functionalities in mobile applications such as in-APP purchasing (e.g. Masterpass API). Paypal and Amazon Payments have both been running a programme for developers who are keen to implement their services. Banking institutions have also utilised external APIs to extend their reach to other platforms and increase their sales by enabling authorised third-party access to some of their services (e.g. money transfers, credit functionality, etc.). Several such examples exist in Europe, North America, Africa, and the Asia Pacific amongst other regions. These range widely in terms of the level of access and control they provide to their infrastructures and which third-party providers (TPPs) they allow to use them. For instance, challenger banks such as Starling Bank in the UK and Fidor in Germany, have used external APIs more aggressively to open up a very wide range of functionality to third-parties and are engaging with independent developers to enrich their API platform. BBVA, an incumbent bank in Spain, was also one of the "first-movers" to provide a developer's portal and authorize TPPs to access its money transfer and other services.

As a general rule, the Euro Banking Association (ABE-EBA) distinguishes between 'closed' and 'open' APIs in banking and provides a spectrum of *open APIs* based on their level of *openness* to third-parties (ABE-EBA, 2016). This ranges from 'partner' APIs accessible only to banks' preferred partners and developers, through to 'public' APIs that are available to anyone (typically after some form of basic registration).

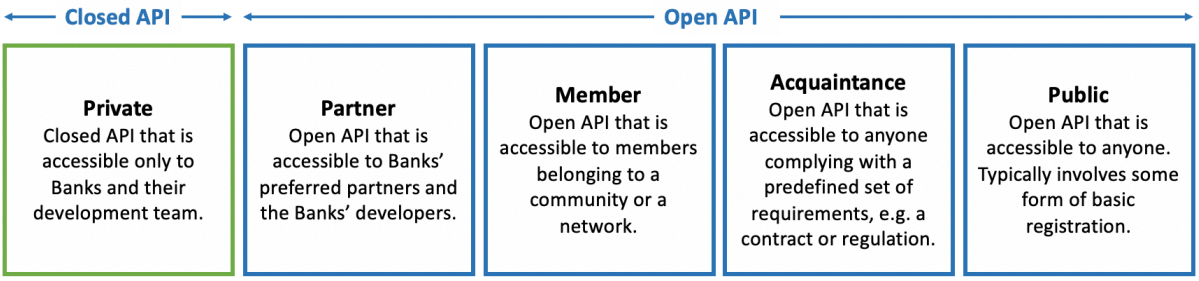


Figure 1. From *private* to *public* – spectrum of API openness based on accessibility (adapted from ABE-EBA, 2016).

The Open Data Institute (ODI) provides a similar categorization around data accessibility in the banking sector ranging between closed, shared, and open data. Based on their interpretation of *open data* as "data that anyone can access, use or share" (ODI, 2016) they highlight that an *open API* does not imply access to open data but, rather, it can be used in closed environments (to facilitate access to sensitive data internally within an organization) or shared infrastructures (to give access to particular group-members following authentication or larger populations subject to license that limits use). Using this definition of open APIs, it implies that 'open' here refers mostly to the *open standards* of the API technology, data formats and even security arrangements used to design APIs (and regulate access) rather than the measure of accessibility of these APIs (the two of them often correlate and this frequently is a source of confusion). As we discuss below, open standard APIs can be key enablers for data-sharing in the industry as they are commonly accepted and easily reused.

Nevertheless, the characterisation of *openness* and classification of interfaces shouldn't be limited to the accessibility point-of-view (i.e. who has access to APIs) or the open standards.

One can also measure openness and classify APIs in regard to the number and modes of interactions they can offer. For example, the type and range of data a third-party can access through an API would also signify how open an organization is to the "outside world". In that sense, a 'rich' API would incorporate much more data (both in terms of number of variables and period of time) and potentially offer more opportunities for new functionalities. Another useful distinction is between *read-only* APIs that only allow read-access to data, and *read/write* APIs that permit users to also make amendments and edit records at the location where the data reside. The latter characteristic can make a significant difference in the way third-party developers can use these to facilitate new products and services. A typical example in banking that utilises read/write APIs is that of the "payment initiation" as this requires a new entry on the original database to update the ledger containing account information of the customer (e.g. their balance and list of transactions, etc.). Table 1. below provides a comprehensive list with the various dimensions of API openness that should be considered when drafting and data-sharing framework in banking.

Table 1. Dimensions of API openness in open banking frameworks

API accessibility	How accessible are the data being shared? Who can access the APIs (e.g. private, partners, members, acquaintances, public)?
API functionality	What categories of data are being shared and what is the level of granularity? How open are these data and how widely can they be shared? How many APIs are there and what functionalities/services do they offer (e.g. read-only APIs for Account Information, read/write APIs for Payment Initiation, etc.)?
API usage	How much data can the APIs communicate and how quickly (e.g. bandwidth of the infrastructure and how resilient it is)?
Open APIs	Are open standards used for data-sharing (this includes API, data, and security standards)?
Alternative APIs	Are diversified data and technologies (e.g. social media and private data, sensor & mobile technologies, etc.) leveraged to provide better access to financially excluded populations?

The move to open banking

While open access to data has proven to provide numerous benefits to the surrounding ecosystem and create value for end customers[5] (Martin et al., 2005), hoarding data for exclusive use can offer significant competitive advantages to a single, or narrow, group of organizations leading to a monopolistic environment – a setting that is very common in

[5] Empirical data have shown that prior regulatory reforms aiming to enhance competition in industries such as transport, telecommunications, and energy have been associated with larger R&D investments, increased outputs, and productivity gains for organizations, as well as, lower price levels, better quality services, and more choice for consumers.

several banking markets globally. Due to poor availability of meaningful information these information asymmetries, more than often, lead to poor market outcomes and are an effective barrier to competition. Ultimately, end customers may be missing out on opportunities to access new and innovative services as there is less of an incentive to innovate in the sector and create meaningful product differentiations. In principle, information asymmetries may also lead to lack of transparency for both prices and quality of services as there is little prospect for consumers to compare between different providers. Independent studies commissioned by regulators such as the Fingleton Associates and ODI report (2014), done for the Cabinet Office and HM Treasury in the UK, seemed to confirm the above negative outcomes for both competition and consumers in the banking sector which opened the discussion for further data-sharing.

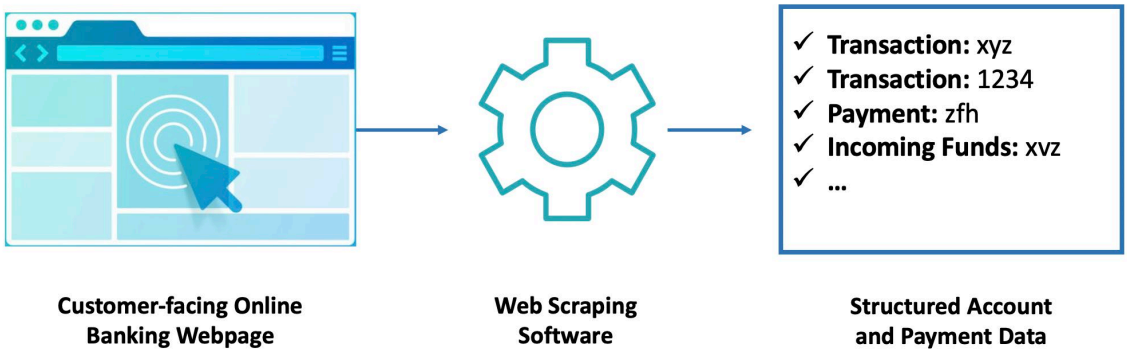
At the same time, there has been a strong demand for data-access from alternative financial services providers such as payment services providers, alternative lenders, financial advisory and comparison services, accounting software firms, and even technology companies (FinTechs and large tech firms alike) aiming to take advantage and extract considerable value from financial data. To satisfy their demand for data, and due to the lack of banking APIs issued by banks, many third-parties started utilizing alternative methods to access information directly from banks through digital interfaces and electronic channels such as online banking websites and mobile applications. This practice, known previously as *data-scraping*, became quite popular leading to an entire market of *screen-scraping* providers (e.g. companies like Yodlee) that offered data-extraction services through "automated, programmatic use of a website, impersonating a web browser."[6]

Box 1. Screen scraping process in banking

Screen-scraping – also known as *terminal emulation* – is a method often used to access and capture data stored in 'closed' systems where information is displayed in such format meant to be readable by humans and not by computer applications. A good example of this is data residing in web sites where a *web scraping* application will 'lift' the unstructured data as they are presented in the web-page and store them in a structured way (e.g. in a spreadsheet format) that can be analysed or re-used. Screen-scraping is not new and has been used extensively, and for many years, in the travel and hospitality industries and for businesses operating product comparison or booking services.

In the context of banking, it is employed to access a customer's banking page and extract their account, transactional, and other data that can be accessed through the bank's online service.

[6] See Tim Rogers, "Screen scraping 101: Who, What, Where, When?", GoCardless in The Open Banking Hub (July 2017), accessed: https://openbankinghub.com/screen-scraping-101-who-what-where-when-f83c7bd96712.



This process naturally requires that the customer shares their login credentials with the third-party provider (TPP) that performs the screen-scraping task so that they can impersonate the user and get access to their account data online. Due to increased demand for information and customers' preferences to share their data with third-parties, screen-scraping gradually became a common practice in financial services. This led to the creation of a niche market of data brokers or intermediaries who would specialize in extracting data from banks (on behalf of the customer) and sell access to third parties (e.g. FinTechs) who would then reuse the information to provide new and innovative services to customers. Such firms such as *Yodlee* (founded in 1999 and acquired by *Envestnet* in 2015) and *Plaid* (recently acquired by VISA) became important pillars of the data-sharing economy in financial services as they facilitated access to data when it was difficult and expensive for TPPs to do so independently.

Banks and large financial institutions, from which screen-scrapers have traditionally harvested data, have raised concerns about this practice and pushed for it to be abandoned. The debate still goes on today in the context of open banking in the EU and other jurisdictions around the world (see more information later in this report). From a FinTech and third-party developers' perspective, screen-scraping can also be costly as it is not standardized and requires constant attention to changes done on online banking webpages which can make scraping data software mismatched. From a user perspective this can also mean delivering an unstable product which can jeopardise the overall service experience.

While this approach can be quite effective, allowing third-party providers to mediate activity on behalf of the end users thus enabling them to perform actions and access information that they would normally do manually on the online banking website, they have been criticised severely from incumbent banks as they require customers to give up their login credentials (e.g. usernames, passwords, piece of memorable data, etc.) and trust them to the third-party. Whereas it is obvious that sharing and storing users' credentials may pose risks (mainly for users but also for the data-scraping service providers), FinTechs, TPPs, and data platforms who benefit from this practice continue to defend their position by showcasing the use of encryption and other security measures while also blaming banks for delaying or refusing to share data through APIs. The extensive application of screen-scaping as well as the discussions around its legitimate use in banking has been one of the most heated debates in

finance and effectively brought the case of data-sharing forward and to the attention of many stakeholders in finance – *open banking* had already begun!

Considering all the above, a number of economies around the world set out to explore opportunities around greater, more systematic, and secure sharing of data in the banking sector and other areas in finance. It was soon acknowledged that a well-formed and effective data-sharing framework would help to achieve many positive outcomes in the sector including a) the enhancement of competition and lower barriers to entry for new entrants, b) access to better and cheaper products and services for consumers, c) access to more innovative services, as well as d) improved financial inclusion for end users especially those who struggle to get access to the current financial system (this applies for both people from unprivileged backgrounds or SMEs with little or a problematic history that do not satisfy the existing banking access criteria). Some regulators have also stressed the fact that the customer-data held by banks inherently belong to the customer, and thus, there must be a systematic way to for them to access it if they wish and share it with third-parties when they consider beneficial.

Even though there is general consensus, in different parts of the world, to carry out the above mandates, these have been dealt with differently by an assortment of public and private sector data sharing initiatives – each with their own approach to consumer access and control over data and digital identity. At a basic level, a data-sharing model should cater for a way to collect and/or create personal data from individuals and give them the opportunity to decide whether and how these data will be shared to third-parties safely (Mazer, 2018). Similarly, one can define that an open banking framework is:

> a secure and standardized technology which, when coupled with rules and procedures, allows consumers to safely create, share, or amend their digital records (e.g. transaction data, payment initiation, etc.) with authorised thirdparties offering products and services.

The above description, while not complete by any means, offers a working definition highlighting some of the fundamental characteristics of open banking. One of its key features, based on the explanation above, is that it creates the platform or infrastructure upon which other participants can build valuable products and services that will make consumers lives better – in that regard it resembles the internet upon which valuable software applications sit. In addition, it provides a standardized interface (most commonly an API) that facilitates the connections between various actors participating in the licensed consortium of firms. Such an interface would normally sit on top of a common rulebook and technology stack used by the entire market which would include important components such as a security protocol so that it can ensure that consumers' data are protected; an identification framework in order to establish the identity and legitimacy of the party on the other end of the interface; and a consent mechanism and permissions dashboard to verify the consumers' accord for the data-sharing activities and allow them to withdraw if otherwise. The complexity of all the above often times creates confusion and misunderstandings around how an open banking framework would function and treat consumers' data. For that reason it is also useful to include a list of what open banking isn't. A brief review of three of the most popular open banking regulatory frameworks in the UK, EU, and Australia follows.

Top 5 open banking myths busted

- Myth 1: "Open banking means everyone will have access to my data!"
  Open banking is a consensus-based and opt-in system that can only be triggered if a consumer agrees to give access to their data with certain authorised entities. Consent can be revoked at any time if the end user chooses to do so and the third-party accessing the data will need to delete all the information they keep.

- Myth 2: "In order to use open banking I will need to share my username and password."
  No customer will need to share log-in credentials with any of the third-parties that seeks access to their data. This is the key strength of open banking that makes is safe and secure for consumers, unlike other methods such as screen-scraping.

- Myth 3: "Open banking is a product that consumers can use."
  Open banking is only an enabling technology and, in and as of itself, does not deliver propositions to consumer and does not provide for any of the financial detriments discussed above.

- Myth 4: "Open banking is new."
  Data sharing in banking has been evolving for at least 20 years. One of the reasons regulators have started thinking about it in a more systematic way is that the business models established around open banking and the value that we can channel to the customers by better enabling better data sharing were deemed quite significant.

- Myth 5: "Open banking is all about APIs."
  Certain regulatory frameworks such as PSD2 do not even mention APIs. Also, an API can never be a business strategy but is only an enabler. One needs to be thinking clearly with a business opportunity in mind centred around the customer – it is entirely customer centric.

Open banking paradigms

UK Open Banking

The United Kingdom has been one of the proponents of open banking globally and the first country in the world to consider such a regulatory move. As such, this is a topic that has been hotly debated between the various stakeholders consuming a massive amount of political capital to discuss its merits, risks, and impact. The first attempt to open up the banking sector through the creation of a data-sharing model was the *Midata* initiative which was launched in 2011 by the Department for Business, Energy and Industrial Strategy (BEIS) [7]. The scheme was designed to allow consumers to compare current accounts and increase switching by providing better access to their transaction data in a portable electronic format. While, in principle, the idea was good, and banks voluntarily supported the initiative, it did not achieve widespread adoption. This was mostly because its implementation was file-based and led to many issues such as bad customer experiences (users had to download and upload files),

[7] See more here: https://www.gov.uk/government/news/the-midata-vision-of-consumer-empowerment.

static information (one-off snapshot), and fraud (customers could edit the data before sharing)[8]. It quickly became apparent that a better and more systematic way should be considered. In 2014, the Fingleton/ODI report done on the behalf of the HM Government, concluded that "greater access to data has the potential to help improve competition in UK banking" and put forward a firm recommendation to use standardized APIs to connect third-parties such as FinTechs, developers, and corporates (2014). An official market investigation by the Competition & Markets Authority (CMA) confirmed that certain features in the UK banking market distort competition and leave banks with "unilateral market power over their existing customer base", thus, leading to lack of innovation as well as expensive and poor-quality services (CMA, 2016). To remedy this situation, the CMA instructed the creation of an implementation entity – the Open Banking Implementation Entity (OBIE) or also known as Open Banking Limited – in order to drive the development and delivery of the "open and common banking standards for APIs" in close collaboration with the industry (CMA, 2017).

As the starting point for UK Open Banking has been the innovation and competition elements, the focus of the CMA order was on the 9 largest banks in Great Britain and Northern Ireland who were also called to cover the costs for the development and deployment of the infrastructure. In addition, pressure around the consumers' rights to their data as well as the security and data privacy risks inherent in older data-sharing processes and technologies, such as screen scraping and card-on-file transactions, were also important factors. In general terms, and with a few exceptions, UK Open Banking mirrors the EU directive on payment services[9] and thus borrows the same kind of regulatory definitions (see PSD2 description below). Having said that, UK Open Banking has a few unique characteristics that make it stand out from other open banking implementations. Firstly, it sets out a single open standard for APIs that provides the specifications that "inform the design, development, and maintenance of an open API" (Payments Forum UK, 2015). Secondly, it provides a governance structure which oversees the standards, ensures that the requests of all stakeholders are addressed, and establishes trust and confidence in the ecosystem. Finally, it owns and maintains a directory of all open banking participants (the "whitelist") which uses digital certificates to authenticate third-parties (TPPs). Open Banking regulation in the UK went into force in January 2018 triggering a "managed roll out" which had to be met until September of 2019.

Payment Services Directive II (PSD2)

PSD2 is a role-based framework aiming to promote the emergence of new players, such as FinTechs, and encourage innovative internet and mobile payments across the EU. This means that actors can hold more than one role. You could be the bank that sends the data out, but a bank can also switch sides and become a TTP providing a particular service and claiming access to outside customer data. PSD2 uses a licensing structure to enable Account Servicing Payment Service Providers (ASPSPs) such as banks and building societies, allow their customers to share their data securely with the authorised TPPs they wish to without the need of contractual relationships. Third-parties are generally either Account Information Service Providers (AISPs), providing consolidated information on one or more payment accounts maintained by a payment service user, or Payment Initiation Service Providers (PISPs) offering an online service to initiate a payment order as requested by the payment service

[8] "Open Banking, Preparing for lift off", Fingleton Associates and ODI report, June 2019.

[9] PSD2, including its associated Regulatory Technical Standards as developed by the EBA, was transposed to UK law through the Payment Services Regulations 2017.

user[10]. As mentioned above, PSD2 does not explicitly require ASPSPs to use APIs in order to fulfil their obligations, nevertheless, read/write APIs are deemed the best way forward to access AI and PI services. To facilitate a safe and secure "access to account" (XS2A), the European Banking Authority (EBA) came up with a set of Regulatory Technical Standards (RTS) or requirements designed to reduce payment fraud and data bridges. This so-called Strong Customer Authentication (SCA) mechanism is a form of two-factor authentication designed to prove that the end-user is he who he says he is. PSD2 and the relevant RTSs apply to all ASPSPs across the EU member states and the regulation went "live" in January 2018.

Consumer Data Right (CDR) in Australia

The Australian approach to open banking has been different from its precursors in Europe. While UK OB and PSD2 focused more on the competition side, Australians had a different starting point looking mostly at the consumers' rights to access and share their data seamlessly, thus, allowing for greater choice of products and services. This permitted them to take a broader view of data-sharing and expand it beyond (open) banking and into the telecommunications and energy industries. While the Australian open banking shares quite a few basic principles with other data-sharing movements in banking – such as consumer-centricity, targeting competition in the sector, creating opportunities for more, better, and cheaper services, and introducing a safe and fair environment – its major differentiation is that it only allows for read-access to data. This means, effectively, that the regulation does not support payment initiation. In addition, the Australian model handles liability and data-sharing obligations differently. For example, it imposes reciprocal obligations to share data and liability is more straight-forward.

Similar to the other schemes, the Consumer Data Right bill mandates that it "is a right for consumers to choose to safely share their data with accredited, trusted recipients [and] it is not a right for businesses to share consumer's data without their consent" (Australian Government, 2018). In Australia, all Authorised Deposit-taking Institutions (ADIs) are mandated to comply with the data-sharing rules. The framework was scheduled to go into force in the finance sector in July 2019 and implemented by the Australian Competition and Consumer Commission (ACCC) that also administers accreditation for participants, albeit more regulators are involved overseeing different parts of the entire enterprise.

Regulating open banking in Canada

Following the global trend and prominence of data-sharing agendas in banking around the world, in September 2018, the Canadian Government announced the launch of the Advisory Committee on Open Banking in order to review the potential merits and feasibility of a banking data-sharing framework in the Canadian market[11]. The review which was also mentioned earlier in the year as part of Finance Minister Bill Morneau's 2018 Budget Plan,[12] was launched in January 2019 with an industry consultation that invited stakeholders to

[10] For detailed definitions see: https://www.openbanking.org.uk/about-us/glossary/
[11] Department of Finance Canada, News Release: "Minister Morneau Launches Advisory Committee on Open Banking", accessed here: https://www.canada.ca/en/department-finance/news/2018/09/minister-morneau-launches-advisory-committee-on-open-banking.html
[12] Government of Canada, 2018 Budget Plan: https://www.budget.gc.ca/2018/docs/plan/toc-tdm-en.html

submit their views. A consultation document[13] providing a brief overview of open banking (described as a "a framework where consumers and businesses can authorize third party financial service providers to access their financial transaction data, using secure online channels") was also published to help participants and the Committee ask the right questions and clarify the review process. The paper posed a number of questions such as: what would be the benefits and improved outcomes that open banking could bring to Canadians and in what ways? How can consumer protection, privacy, cyber security, and financial stability risks be managed? What would be the appropriate role of and steps that the federal government should take in implementing open banks? Beyond the written responses submitted (approximately 100) by the organizations and people who took part in the consultation, the Department of Finance along with the Advisory Committee also ran a number of roundtables and discussion sessions across Canada in order to collect the industry's opinions on the above themes. Overall, hundreds of stakeholders participated across Canada representing around 140 institutions[14].

Trailing the Government's consultation process, the Standing Senate Committee on Banking, Trade and Commerce also released a report[15] looking at the challenges and opportunities of open banking in a Canadian context. The report, which reinforces the message that the control of the personal financial data "should lie with the consumer and not with the businesses that collect it" (p. 37), puts forward a number of immediate and long-term recommendations that the federal government should consider in order to launch a robust and successful open banking framework. These largely include calls for the development of a principles-based industry-led open framework, the involvement of consumer protection groups in the process, the designation of oversight bodies and regulatory enforcement authorities, and the modernization and alignment of existing privacy and consumer rights regulations with global standards. These recommendations were published after meeting with and accepting written submissions from several national and international market experts (including bankers, financial services professionals, technologists, consultants, policy-makers, etc.), industry bodies representatives, academics, regulators, investors and other stakeholders. While the sample-size of this exercise was sufficient (39 people were interviewed and 11 participants provided a written submission) it wasn't particularly representative as only two or three individuals were largely expressing the voice of the FinTech startup and Challenger Banking ecosystem in Canada. Nevertheless, the report's key message was quite positive and urged the government to act rapidly and "decisively" to bring open banking to practice for the good of the consumers and the industry.

More recently, on the 31st of January 2020, the Department of Finance Canada released the findings and recommendations of the Advisory Committee on Open Banking following the public engagement with Canadians and financial services stakeholders. The document which was called "Consumer-directed finance: the future of financial services", focused more on the consumer protection, privacy and cybersecurity risks of open banking, also renaming the initiative "consumer-directed finance" to avoid any misunderstanding around what openness

[13] "A Review into the Merits of Open Banking", Consultation Document, Department of Finance Canada, January 2019. Accessed here: https://www.canada.ca/en/department-finance/programs/consultations/2019/open-banking.html

[14] Full list of stakeholders that participated in public engagement can be found in Annex A here: https://www.canada.ca/en/department-finance/programs/consultations/2019/open-banking/report.html

[15] Standing Senate Committee on Banking, Trade and Commerce, Senate Canada: "Open Banking: What it means for you", June 2019. Report accessed here: https://sencanada.ca/content/sen/committee/421/BANC/reports/BANC_SS-11_Report_Final_E.pdf

implies for consumers and to be more descriptive on what the proposal involves. While the document embraces data-sharing and highlights its benefits in the context of banking it provides very little discussion around some of the hottest topics in the open banking debate which leaves for the next round of consultation: "the Committee and Department intend to explore in greater depth some of the themes raised by stakeholders in the context of the roundtables, among them: liability, accreditation, governance, the question of how screen-scraping should be dealt with and how to build an ecosystem that is accessible to all participants." (Department of Finance Canada, 2020).

Considering the level of open banking discussions in Canada and access to extensive amounts of information and knowledge from implementations in other countries, the public debate is somewhat ahead of the official Government consultations and not focusing as much anymore on the "merits of open banking" or opportunities that it will bring. Indeed, many commentators feel that "this line of inquiry feels very old" and is a "time-wasting rabbit hole"[16]. Instead, industry stakeholders and regulators should try to shape up a clear objective to drive industry and consumer participation and attract investments into the market, as well as discuss what version of open banking implementation would fit best the Canadian market and assess its feasibility (something that was allegedly underestimated in the UK and the EU).

Following exploratory conversations held before the commencement of the study, it became immediately clear that such questions did not have straight-forward answers and also carried a heavy load of unresolved economic, political, financial, regulatory, and sociological issues and conflicting views between key stakeholders whose interests were threatened or advanced. This study attempts to shed some light on the key themes, conflicts, debates or frictions that will shape the impending open banking framework in Canada.

Research design and methodology

To study the potential drafting and implementation of an open banking framework in the Canadian banking sector and explore the risks and opportunities as well as competing views that this could introduce, a *qualitative* study was deemed as the most suitable. Qualitative or *intensive* research methods such as interviews, archival studies, ethnography, case studies, and observations are generally considered "epistemologically valid" (Tsoukas 1989, p. 556) and can provide rich, empirical descriptions of particular phenomena. Researchers can use such data to identify structures and interactions between complex mechanisms and construct a comprehensive picture of the various socioeconomic, political and other dynamics that may influence the final outcomes (Layder 1990; Sayer 2000; Volkoff et al. 2007).

In order to be able to identify (demi-)regularities in the various narratives concerning the risks and opportunities of open banking in Canada, this study conducted a considerable number of interviews as well as roundtable discussion observations and document analyses from a variety of sources. To keep a balanced perspective between the various stakeholders, it was deemed necessary to capture arguments from four main groups of people/organizations: (i) *FinTech* startups and *Challenger* (or *Neo*) Banks, (ii) large *incumbent banks* and deposit-taking financial institutions, (iii) industry experts (e.g. consultants, legal experts, investors, industry association representatives, etc.), and lastly (iv)

[16] Samson, Dominique (2020), "Open Banking: Canada Might Not Be Able to Make Up for Lost Time" accessed here: https://debanked.com/2020/01/open-banking-canada-might-not-be-able-to-make-up-for-lost-time/

regulators and government bodies. Table 2. lists the number of individuals that were interviewed from each one of these categories of people and institutions.

Table 2. Sample description

(i)	*FinTech* startups & *Challenger* Banks	11 interviewees from 7 organizations
(ii)	*Incumbent* financial institutions and Banks	13 interviewees from 4 organizations
(iii)	Industry *experts*	13 interviewees from 8 organizations
(iv)	*Regulatory* and *government* bodies	20 interviewees from 5 organizations
	Total numbers	**57 interviewees from 24 organizations**

The roles of the individuals interviewed varied according to the organization or institution they represented. The norm was to target senior professionals who would have the experience and knowledge to understand open banking and its consequences for their business at an operational, technological and strategic level as well as be part of the industry discussions representing their firm. Some of the roles of the people interviewed were CEO, Co-founder, Vice-President (VP) of Innovation, Chief Strategist, Chief-of-Staff, Managing Director, Head of Legal, Partner, Head of Research and Strategy, Chief Information Officer, Director or Policy, etc. Head of Technology, Head of Regulatory Affairs, Senior VP for Innovation, Director of Strategy, Senior Legal Counsel, etc.

The interviews conducted were mainly semi-structured allowing for a number of questions (narrow as well as open-ended) to be asked from an interview guide but also accounting for the diverse expertise and background of the interviewees. All informants were asked to provide some basic background information about themselves and their careers as well as the organizations they work for. They were then asked more specific questions about their perceived risks and opportunities around open banking. Most interviews lasted between 60-90 minutes and extensive notes were taken during and after the sessions to capture the entirety of the discussions[17]. In addition to interviews, company documents (mainly presentations and consultation responses), government and other press-releases, regulatory texts, and media articles were also collected to supplement the material communicated during the interviews and to cross-check/validate claims of the interviewees. These were used as secondary and supplementary data and thus we did not perform a systematic data analysis. Finally, the research investigator had the opportunity to attend 6 conferences and roundtables during which he had the opportunity to ask questions and clarify positions with other event

[17] For some of the interviews, research participants were asked to be recorded and transcripts of the discussions were used in addition to hand-written notes.

participants. This was a very effective way to obtain answers fast and refocus the questionnaire towards more interesting topics while also expanding the research network and setting up more interviews. The overall duration of the data collection exercise lasted 6 months (between February 2019 – July 2019) with another 6 months (between August 2019 – January 2020) of data analysis and write up of the results and of the paper.

Below we attempt to identify the various **key themes and debates around developing an open banking framework in Canada** and present views and perspectives that stakeholders brought forward while discussing the risks, 'pain-points', and opportunities that an open banking framework would introduce to the Canadian banking industry and to its customers. Considering all the interviews, observations and documentation analysis, the research identified ten different themes that seemed to be of key concern to practitioners and regulators alike. These were grouped under four main categories: 1) objectives of open banking in Canada, 2) regulatory issues and the Canadian context, 3) creating a data-sharing infrastructure, and 4) participant goals and concerns. The views that were expressed vary depending on the background and incentives of the different interviewees in our sample. They are often contradictory.

Key themes and debates around developing an open banking framework in Canada

Objectives of Open Banking in Canada

Policy-mandated vs. market-driven: drawing on UK and Australia paradigms

Two of the most critical decisions that need to be addressed regarding the design and implementation of an open banking framework are: (i) what is the overall *objective* of an open banking framework order, and (ii) whether this is going to be driven by a mandatory (regulatory) compliance order or a voluntary, industry-driven scheme. Evidently, both decisions are going to affect the speed and extent with which data openness will happen in the sector. Of course, such decisions will vary between contexts. A strong policy mandate and a convincing socioeconomic argument on why the economy needs open banking, and what the potential objectives and benefits for consumers are, can go a long way in realising an open banking framework. Having said that, a government-driven policy, though mandatory, can be slow to draft and impose especially if the mandate is broader and involves several industries. A private sector-led policy can be more flexible and adopt novel approaches to standards and data-sharing that are harder to draft. In the latter scenario the incentives to adopt would be triggered by peer-pressure and competition in the market rather than a regulatory framework. In addition, it is important to figure out the level of involvement from the industry and/or the public sector in designing and running the infrastructure and maintaining standards as well as covering the costs.

There are several examples that resemble the above scenarios depending on the context and market structure at the time. As discussed above, in the United Kingdom, the origins of open banking were mostly grounded in the competition narrative and the need for greater access to data in order to help improve the sector as per the findings of the Fingleton/ODI report (Fingleton, 2014). This was, also, the main reason Open Banking in the UK was "ordered" by the Competition and Markets Authority rather than by some other data privacy-related regulator. On the contrary, Australian regulators approached open banking from a data-rights

perspective and regulated data-access through the Consumer Data Right bill. As one of the Australian regulators communicated during the course of this study:

> *"it's not about the banks, it's about the Australian customer […] the policy is about looking after the data of the customer."*

This has been the guiding principle for the Australian open banking regulation which mandates that people and businesses should have the right and means to share their data with whoever they wish (subject to accreditation). Unlike in the cases of Australia or the UK, our findings show that the Canadian context does not currently seem to provide a clear narrative concerning the grounds according to which Government should pursue (or not) open banking in the country and how. As senior figure of a *Neobank* admitted:

> *"open banking potentially can be very much a pro-competitive force but the Department of Finance's call is not entirely clear what their objective is"*

adding

> *"maybe in Canada we can muddle along without necessarily having a purist view […] there is a feeling [however, that] there is not enough competitive intensity in the banking system and as a result, consumers are not getting good enough rates on their deposits, interchange fees and credit cards are too high, mutual funds fee are high – obvious things that could potentially be solved with a bit more competition."*

Indeed, some of the study participants in our sample (especially from the "*FinTech* startups & *Challenger* Banks" category) had a similar conviction that the Canadian banking system needed more competition to battle expensive fees and increase the quality and originality of products and services of their consumers. Speaking of the Canadian banking environment, another FinTech co-founder highlighted the problem of little competition and argued that:

> *"it's because we have a highly protectionist environment which has focused on stability to the detriment of competition in a pretty myopic way."*

A number of questions ascend from the argument above. For example, how is increased competition realised in the industry, and how can banks "feel the heat" through sharing customer data? For some regulators around the world, account switching figures are a natural metric or KPI to assess the effectiveness of data-sharing initiatives. A small number of interviewees however challenged this idea as irrelevant for the Canadian context:

> *"the Canadian competition people seem really hung up on this idea about switching, which to me this feels like a real red-herring. At least in this marketplace there is no FinTech that wants to offer deposit accounts […] nobody wants to be regulated as a bank in Canada if they can avoid it. So, this idea of promoting competitiveness because you want switching just seems like very much not consistent"*.

In addition to the narrative around competition, a number of participants added that open banking is a good opportunity to prioritise consumers and be more "customer-centric". Having said that, this argument can also be misleading as it is very different from saying that the customer:

> *"gets to decide and have the ability to direct their preferences around the economy [through data-sharing] without any limitation because it's his data"* (as a technology consultant shared)

which is something that points more to peoples' data-right. Finally, in addition to observations around competition and customer-centricity, a category of study participants

also expressed a different view around the dominant reasons for the open banking efforts. A legal expert said:

> *"I think [the reason Government is considering open banking] it's to keep up with other jurisdictions, that's why they are doing it"*.

During most discussions there was also a sense of urgency when comparing to other countries who are ahead in implementing similar frameworks. As a FinTech representative expressed:

> *"The conversation has come to Canada the last 6 months but it feels like we're so far behind the UK"*.

Many of the people in that group, however, questioned if the argument of "fear-of-missing out" from international developments was a valid incentive to follow through with such a rigorous industry transformation. Following the objectives above, an issue that was frequently mentioned, as a barrier for open banking adoption in Canada, was the customers' perception of the benefits and opportunities that data-sharing would bring. Many industry practitioners pointed to end-users being hesitant or misinformed. In that regard, a venture capitalist focusing on FinTech investments commented:

> "*To gain the political support and public support we need to reframe the story […] we think the word open banking as a concept does not resonate with the public. However, if you reframed and repositioned it as consumers banking right, I think there is no Canadian that wouldn't say 'that sounds like a good thing for me'*."

Following the argument above, an industry expert also mentioned that:

> *"this is the struggle! If you look at the consultation paper, I've never seen a consultation paper look like this. It was more like a PR piece for consumers […] so they clearly try to sell it to consumers who until now they've never heard of open banking and aren't really motivated to push for anything."*

In line with the above, a study that was commissioned by the Department of Finance found similar results. The research, which was based on qualitative insights from consumers, concluded that "the concept of Open Banking is unknown and the name conjures a negative association to most participants. The description of Open Banking is confusing" (p.8)[18]. Whatever the objective of the framework, regulators will still need to decide on whether a voluntary-based or a mandatory regulatory scheme would be better and more effective in triggering the desirable outcomes in the market. A senior figure and investor close to the FinTech world discussed:

> *"Our perspective is that in Canada, given the market construct, it has to be a policy-led initiative […] without policy the banks won't be moving on it or they will move on it in a way that it's in their best interest"*.

While this opinion was shared by quite a few interviewees there was agreement that a decisive regulatory order would need to be backed by a strong political will – as a source commented:

> *"You need a political champion"*.

Lack of a grand governmental plan to regulate and implement a data-sharing framework can lead to delays but also adverse outcomes from the industry.

[18] "Open Banking Qualitative Research Final Report" Pollara Strategic Insights, March 2019.

"Our government is quite innovation-focused and they have certainly prioritised this, it's just that we are slow to regulate and innovate from a regulatory perspective. We like our financial system stodgy and boring and predictable".

Regulatory issues and the Canadian context

The liability issue

One of the main reasons certain governments and regulators choose to move towards a policy-driven mandatory data-sharing rulebook is due to issues around the obligations in the relationship among the different entities that handle customer data. In an open data-sharing environment one should be able to answer questions such as: "how do we make the customer whole in case something goes wrong with a payment?", "how do we know the customer consented to having their data shared?", "how do we know which entity lost the data?", etc. According to PSD2, in the payments use case, it's always the bank that will make the customer whole in the first instance. They will then have the opportunity to turn to the FinTech and challenge them for the wrong practice (e.g. generated a false payment or made a mistake, etc.). For this reason, PSD2 requires FinTech and TTPs to have liability insurance in place in order to be able to pick up the costs of fraudulent payment initiations.

One thing, though, about insurance is that the insurance companies under contract will not pay out unless liability can be established. Taking this into account, any regulator who is keen to put forward a framework of a workable open banking regulation, will need to start from that position. A solid directive must be able to help assess and trace who the "bad actor" was in the chain as there may be multiple actors holding the data. For example, in the account information services space the liability model is reversed. When the data has been transferred to a regulated actor and are now at rest in their system, it is the regulated actor who has to make the customer whole if something goes wrong and the data is breached, and not the bank. One of the incumbent bank representatives in Canada highlighted the above issue:

"banks have no control over what the [account data] aggregators are doing with this. So it's actually a security risk […] if one of these aggregators, which maybe have 200,000 customers, if they get breached where is the consumer going to go?"

The banks' obligations are satisfied as long as they have fulfilled two key conditions: firstly, the data must be communicated with a regulated actor, and secondly, they have to make sure that the end customer consented for the data to move. Various interviewees in our sample seemed to express similar views. A legal expert, acknowledged that even if a potential open banking legal framework in Canada clearly addresses and articulates the liability distribution across parties:

"there needs to be an ability, either through insurance or some other method, to actually withstand that liability".

In that context, another legal representative of a FinTech also shared that:

"You certainly need some form of standards in terms of ensuring that there is proper cyber security, at the very least, or operational risk governance more broadly, but you also need either insurance or capital requirements or some sort of financial ability there to take on the risk that is being added into the system. It's much better to set out a framework rather than wait for the courts to figure it out. At the end of the day if it's the courts and you've got some poor individual consumers hit, and there is a bank with a tonne of money […] public perception will surface […] the system is such

that the deepest pockets are always the ones that pay and ultimately backed-up by the Government. There is no other outcome possible".

An incumbent bank employee similarly added:

> *"FinTechs typically just don't have the financial resources to be the real target of any sort of class action for example, so at the end of the day if there is a failure everyone is going to sue the bank, even if the failure was really somewhere else."*

In general, there was consensus amongst research participants that the liability should be structured and controlled in a way that removes the fiscal burden from the customer and also protects the customers from getting into a legal ordeal when things go wrong. In addition, most FinTechs argued that there should be a way to keep barriers for new-entrants to a minimum in order to encourage innovation – the following quote represents this view:

> *"having insurance that re-distributes the risk through the system, through policy holders, etc. premiums to be paid amongst those that do not belong to the class of the deepest pockets – although you don't want to prevent parties from accessing the system if they have the technical wherewithal to add value to the system – there is a lot of competing considerations to take into account."*

Overall, as both payments fraud and data breaches in banking will be unavoidable (especially in the context of open banking), a comprehensive and systematic liability framework (i.e. accessible to everyone and not creating barriers to entry for smaller TPP businesses) is of immense importance for a sustainable and fair open banking implementation. This is also one of the main reasons to pursue a policy-driven data-sharing agenda in Canada instead of a market-driven framework that may create further imbalances between stakeholders. While, the current "consumer-directed finance" government report partially acknowledges the issue of liability, it provides little direction on what should be done and how. It is evident that more work needs to be done in that direction that considers the voices of all the stakeholders as well as legal experts.

Regulatory setting and data-privacy laws

As open banking frameworks have customers' data at heart, it is important to ensure that these exist in parallel to data privacy regulations that sufficiently safeguard the consumers' rights. When this is not in place, there needs to be a programme of bold regulatory transformation in data privacy laws to make sure that consumers are not left "at a higher risk of harm"[19] as data openness in the sector is implemented. In the case of Australia this was the main reason open banking was delayed and pushed several months later in 2020. In the European Union, the General Data Protection Regulation (GDPR) Directive is designed to harmonize data privacy laws across the EU and protect citizens' data privacy. Characterised as "the most important change in data privacy regulation in 20 years"[20], GDPR obliges entities that store and process consumer data for commercial purposes to (1) acknowledge that the data belongs to the user and (2) award them the right to choose how these will be used. GDPR is complementary to PSD2 as it forces TPPs as well as banks to handle customer data responsibly keeping customer transparency and customer data control at the centre.

---

[19] Prior to the launch of the Australian open banking framework, the Australian Privacy Foundation (APF) claimed that the Consumer Data Rights Bill privacy safeguards were not adequate, and that "risks have been severely underestimated by the Government", (see http://www.privacy.org.au for APF's submission in response to the CDR bill).

[20] See GDPR official webpage for more information: https://eugdpr.org/.

The Canadian regulatory setting is somewhat more complex and difficult to bend than in many other countries. This is mainly due to the strong influence of provincial regulators (10 provinces and 3 territories) that leads to considerable fragmentation in terms of legal frameworks. While there are a few federal laws around financial services (such as the *Bank Act*), provincial regulations can be found to be in conflict among provinces as well as with federal laws which leads to further complications. A legal expert in our sample explained:

> *"The struggle is the federal/provincial overlay. Essentially, we have regulation that is piecemeal: it's province by province, some are federal, some are provincial, and it's very difficult initially for a FinTech to understand where they fit in all of this so we don't have that kind of streamline like the FCA model [in the UK]. And we have tensions between federal and provincial, and we have tensions between provincial themselves."*

This regulatory arrangement makes it more difficult to create and oversee a coherent national data-sharing framework as it will be challenging to implement across all regional jurisdictions in Canada in order to work for all financial institutions (banks and non-banks like FinTechs). In addition, there seems to be a challenge around which regulatory body would be the natural candidate for this job. The fact that there is uncertainty around the objectives of a possible open banking regulation in Canada also suggests that it will be hard to align the regulatory activities with the incentives and aims of regulatory bodies – unless significant changes are made. A technology expert, who studies regulatory change closely, mentioned that:

> *"OSFI at this point in history is adamantly pushing back on any attempt to expand its mandate beyond purely prudential […] so, we don't have any comprehensive conduct regulator, and the question is where does any of this* [open banking activity] *fit?"*.

Many other participants spoke about the challenges of the provincial and federal systems and the fragmentations that this structure brings. A lawyer actively consulting in this space commented about the same issue:

> *"This isn't an inconsequential thing, it needs to be figured out. None of these mandates are sacrosanct, like they can't be changed, but no one has really any idea how any of this is going to come together. We've had this experience in Canada of spending the last 15 year trying to get a national securities regulator and it took going to the supreme court with court challenges from Quebec and some other province".*

Navigating and regulating in this context will be a challenging job for the government which will issue the order and for the regulator who will take on the task to draft the bill. A key figure in the industry who largely represents the voice of FinTechs mentioned:

> *"I think the bureaucrats would love to find a way to create policy that doesn't require coordination between the two* [provincial and federal settings]*,* […] *if you do a data right and somehow tie that into some financial regulation without it touching the bank act or OSFI or touch the provincial regulators that would be ideal – but threading that needle is pretty hard."*

At this point, a considerable number of the interviewees suggested that the Personal Information Protection and Electronic Documents Act (PIPEDA)[21], would be a good place to start thinking about open banking reforms. After all, banking data are essentially personal data and any initiative that considers mobilizing these should address how these data should be protected in order to safeguard consumers' privacy. A participant acknowledged:

> *"We believe that probably the best place to start is an update of PIPEDA, which is the privacy act."*

The question, however, is whether this approach would be enforceable across all players and local authorities in an open banking framework. An investor, interviewed about this, shared his thoughts:

> *"And so, if we are going to update our privacy act we think, creating some data right, could potentially be enough to force a market solution – still probably sceptical – but would be interesting to see if that would be enough to get people going."*

In any case, going forward down that path would require strong collaboration among the various stakeholders in order to identify ways to "stitch" financial and data-right regulatory frameworks together. A study participant, working for one of the relevant regulatory bodies, recognized:

> *"We do have privacy legislation that is seen as "GDPR-light", we have a federal legislation, we have two provinces that have their own provincial ones that are similar. The privacy commissioners haven't been too much a part of the banking discussion yet, and they would be the ones that will that* [need to embed] *consumer right to their data frame of reference."*

Incumbent bank participants in our study were also keen to highlight the regulatory challenges and suggest that legal frameworks can go only so far in introducing change in the market. Many of them took this opportunity to argue that an industry-driven (and not a law-driven) initiative would qualify best to push open banking in Canada:

> *"We do have a privacy law that could be used as a basis for the* [open banking] *framework that already exists, and I would say that the privacy law is already regulating open banking and with the* [Canadian] *Digital Charter[22] and the proposed changes for the mobility of data under PIPEDA - that is entering the space of open banking. But it's those other areas that go beyond that are the trickier ones that are really difficult and you would have to look to the market to fill in those gaps."*

From their point of view, the banks are worried that regulating open banking federally could mean that data-sharing requirements would apply mostly to them (as they are already regulated federally through the Bank Act and easier to identify) and not to the whole market

---

[21] The Personal Information Protection and Electronic Documents Act (PIPEDA) is a federal law that addresses data privacy and governs the use of data and personal information by businesses in Canada. Following the launch of the Canadian Digital Charter (discussed below), legal frameworks such as PIPEDA will need to be modernized in order to reflect the principles of the Digital Charter and help strengthen privacy. In line with that, it will have to increase peoples' control of their own personal data, and enhance its enforcement and oversight among other things.

[22] The Canadian Digital Charter was announced on the 21st of May 2019, by the Minister of Innovation, Science and Economic Development, Navdeep Bains. It entails a number of principles that layout the foundation for establishing trust in the digital economy and protecting peoples' data as well as giving them better access and more data rights and control. For more details see here: https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00108.html.

(e.g. all third-parties financial services, and other non-bank institutions that are active in the banking space generally), and so there is a significant risk of creating an "unfair imbalance of control". A senior banking figure argued:

> *"If the government were to move forward and mandate certain requirements on banks [at the federal level] they are leaving out all the provincial regulated financial institutions. Who will be regulating the FinTechs?"*

According to incumbent bank representatives, the government can draw some of the principles and guidelines and let the market decide all the details in a way that works best for the market, customers, and competition. This is already happening with principles-based privacy legislation in Canada which includes, for example, some principles for customer consent regarding how their data are being used. However, a key question here is whether banks are doing a good job in integrating such principles into their processes and interpreting them into technology. For example, are deposit-taking institutions in Canada ready to respond to customer queries around supplying customer data back to the customer? Or, what are the frameworks they use to extract informed consent from their customers? In that respect, one of the legal experts interviewed testified that:

> *"right now banks have been relying on former customer agreements, user agreements, and consents that are outdated – they don't reflect today's reality, they are not as dynamic. They assume that this is a blanket permission to do whatever the bank needs to do with the client's data and that's not the case anymore. As a matter of fact, the* [Privacy] *Commissioner[23] provided clarification on the fact that these things are not static,* [but] *they are dynamic and informed consent is very granular and there are principles such as minimalism that need to apply to such things when you update a consent. That's a challenge. I can tell you none of the banks are ready for that at this point."*

Following the above, banks have been accused of doing the very minimum to comply with tentative rules and try to interpret legal principles in a way that is convenient to them. Having that in mind, many FinTech and Challenger Bank representatives were concerned that this will be the case for any version of an open banking directive going forward. They also worry that bigger banks will influence, in a disproportionate way, the shaping of the ruling as they are the ones with the most to lose. A co-founder of a FinTech startup said that:

> *"[banks may end up dictating] yes, we are doing open banking [but] 'here is the data you can access', 'screen-scraping is now illegal', and 'everything is done in this way'."*

Creating a data-sharing infrastructure

Data openness and competition

As discussed earlier, the level of openness in the sector is arguably one of the most significant themes regulators will need to consider when drafting a regulatory framework for open banking (see discussion and Table 1 above with the different dimensions of openness for open banking). As expected, the debate around openness will be largely influenced by the

[23] The Office of the Privacy Commissioner of Canada is a non-partisan agent of the Canadian Parliament who oversees compliance with the Privacy Act as well as PIPEDA. The Commissioner functions as an ombudsman and investigates complaints brought forward by Canadians who think their privacy rights have been violated. According to the Government's recent recommendations, such model is outdated and does not incentivize compliance, especially in the context of the digital economy. See here for more details: https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00107.html.

nature of the mandate and will apply much less in the case of voluntary data-sharing models where change will be much more market-driven. The level of openness and type of data-sharing in the banking sector will also influence the dynamics of the competition in the sector. This is one of the most obvious reasons why incumbent banks world-wide are not particularly keen to see any open banking regulation. A FinTech representative commented:

"if they had the choice they would never opt for any of that"

Discussions with industry experts reveal that incumbent financial institutions have been quite uncomfortable with the idea of opening up customers' data and will try to do anything to lobby for a "soft version" of open banking that suits their interests. This is also because it is more challenging for incumbent banks to navigate their thinking towards building a technology strategy that fits the digital age and so may find themselves disadvantaged in the mid-long term. An investor and FinTech board member discussed:

> *"It will take a while I think to see a shift of a mindset from 'this is a cause for concern because we are diluting our influence in the marketplace' to 'this is an opportunity to create new products and services'".*

Another FinTech representative mentioned:

> *"That's the interesting thing that there is a huge opportunity with open banking but the banks seem to be more fixated on 'oh, we're just going to become dump utilities' but that to me is the defeatist attitude – I mean you have all of the resources, all of the means, all of the know-how to actually lead in this space. The fact that you choose to adopt this defensive posture suggests that innovation and offering clients better products and services at a lower costs is not high in your priority list".*

Based on the above observations, incumbent banks in Canada are already trying to negotiate their way into benefits that will put them in a better position once open banking arrives. A legal expert and advisor described this:

> *"I think they will use the opportunity of open banking for quid pro quo on expanding on the business of banking. They are going to say 'if you are allowing FinTechs through open banking to do what we do then you will have to let us expand our scope of services as well'. And that's already happened".*

He went on to describe that certain regulatory amendments took place in 2018 that allowed banks to broaden and expand their business scope and services:

> *"it's no coincidence that [this] is happening at the same time as open banking […] there are changes that made it easier to acquire FinTechs for example […] or broaden the kind of business they can do".*

For example, there is an explicit reference to banks being allowed to provide identification and digital ID services going forward.

> *"So the banks are always trying to negotiate with Finance to get certain term so they may comment in certain ways to get some cards over here so that they can get some other benefits over there".*

Another topic that was really central in the discussions with many of the interviewees was around the payment initiation leg of open banking and whether this would introduce further competitive turbulence or additional risks in the sector. Many of the FinTechs in our sample advocated that the inclusion of payment initiation in the open banking framework would significantly challenge the status quo in banking:

"In some respects access to the data it's not of no value, but to me to have another party saying 'pay this amount from this account to somewhere else' then that's where really crazy stuff begins to happen. Banks in some respects become more like utilities unless they can be the ones providing these valuable services."

Another FinTech CEO said:

"From our experience, the most use cases we see are payment use cases that trigger the transfer of funds. […] this is what we are mostly worried about, how will the government be able to standardise what data [e.g. payment initiation in addition account data] rather than like how to access it [that can also be dealt from the market]."

Some, however, thought that it may be more effective to take things slower and make sure things get done right in a gradual way. A FinTech representative said:

"we're still a long way from anything real happening in Canada. I would love to see open payments innovation. I think, all things being equal, it probably puts more jeopardy into the open banking to have the scope increase that much and I'd treat them as separate conversations […] I just don't have enough confidence in our governing bodies to navigate – there's just a lot of moving parts if we make this a multivariable equation".

In terms of introducing further levels of openness (i.e. payment initiation) to break up the competition, some of the interviewees highlighted that open banking in Canada can't be "an end in itself" like in the UK "where they really tried to reduce the dominance of the high-street banks" due to the political climate after the financial crisis:

"the point should be that if they are going to lose market-share these 5 [largest Canadian banks] it should be because there is something better [i.e. further FinTech innovation], and that we shouldn't do anything that gets in the way of that something better coming to market, because if there is something better, then people should have access to it."

While this is a logical argument to make, it is also a chicken-and-egg story since FinTech innovation and investment is largely dependent on regulatory and market conditions in the first place. A regulatory trigger can always be tested to introduce more innovation in the sector. Research largely supports the positive effect of regulatory interventions in terms of promoting innovation but it is too early to say if open banking frameworks, in the EU and the UK for example, had the desirable effects so far. In addition, it is difficult for a third-party data-sharing model to flourish unless there is support for FinTech investment and entrepreneurs in the market – this is because the less FinTechs start-ups exist to take advantage of data-openness, the less effective the open banking framework will be (but also vice-versa).

Digital Identity

Similar to the above discussion around TPP identification, establishing an integrated digital identity for consumers is also an important premise for open banking in order to successfully identify customers and get their consent. Consolidating the digital profiles of an entity (either a retail consumer or a corporate client) can allow for a secure and unified authentication experience. While a complete digital identity solution (i.e. a reference data standard, unique identifier, or address, etc.) may not be directly provided by the open banking system, this

should be empowered through a "ubiquitous authentication mechanism that consumers can use to access their digital identity regardless of where it is stored" (Fingleton, 2019).

In Canada, a step towards facilitating future solutions took place through amending the bank act to allow banks to provide identification services. At the moment there are a few examples of initiatives on digital identity. Perhaps the most popular, mentioned by a few people in our sample, was the Verified.Me service. This started as a joint initiative among Toronto-based company SecureKey Technologies Inc. and Canada's 'big 5' banks.[24] It provides a network solution for digital identity to help bank customers (who already have a verified account with their bank) to confirm their identity faster and more securely without having to repeatedly share information with various third-party "service providers". SecureKey Technologies capitalized on their experience in building a similar solution (SecureKey Concierge service) for the Canada Revenue Service where they used banking credentials to help consumers get easier access online. The service uses IBM's Hyperledger Fabric blockchain technology to ensure that, when transferred, personal data are only shared with trusted network participants with peoples' consent.

A few research participants referred to SecureKey's Verified.Me solution as "interesting" providing certain benefits to consumers and banks:

> *"[it is] relying on a third-party identifier which is typically a bank, so you can essentially check that another bank has KYCed that customer. It's still in a fairly initial stage in Canada but you can see it expanding as a new business line for banks to essentially KYC everyone and everyone [else to] just rely on their KYC."*

Considering the above solution, a few challenges can be foreseen regarding its governance. For example, who is going to be part of this network and who decides that? Will this be open to Challenger Banks and FinTechs so that they can also take advantage, both from the "service hosts" side (i.e. Financial Institution Identity & Data Providers) or the "service providers" side (i.e. firms that request access to data in order to provide services)? Also, how can one ensure a certain quality of on-boarding practices and KYC processes and avoid data quality and fraud issues in the network? One interviewee with tech background who is an expert on the KYC space shared this concern:

> *"…who is the weakest link in the network, for KYC practices? Because there is compliance and then there is compliance. The Office of the Super-intendent of Financial Institutions [OSFI] does examinations and they get differing scores on their risk management practices."*

Even though the above initiative is evidently a good start considering a market-driven solution, it was criticized by quite a few FinTech and Challenger Bank representatives. In particular, there were concerns about attempts from incumbent banks to try and control the system and orchestrate activity for their own benefit:

> *"Digital Identity is also something fed into the schema [of open banking]. But again, the big banks are trying to own that as opposed to providing a federal system so we are basically saying that there should be some kind of sovereign system of Digital ID."*

[24] Initial participants at the time of launch (approx. 1st May 2019) were CIBC, Desjardins, RBC, Scotiabank, and TD, with BMO (Bank of Montreal) following soon after and National Bank of Canada in line to join soon. As of January 2020, Verified.Me counted 11 participants including data bureau Equifax Canada and life insurance company Sun Life Financial (see here for more up-to-date information: https://verified.me/about/#participants).

Another FinTech co-founder criticised the Verified.Me initiative discussing how she thought the market and consumer expectations were higher that what was delivered, which also led to usability and adoption issues:

> *"[…] It's very slow, it's very expensive, the user experience is super bad and really their focus was connecting directly with banks without taking case of the user experience."*

They then added:

> *"[…] what we are scared of is that, since that company got funding from most of the banks, it's a good showcase of a failure of open banking in Canada, and […] this could potentially be used as a bad example [of showing that there is no demand for open banking services]"*.

Hopes for a centralised, shared, and 'universal' digital ID initiative are generally hard to be fulfilled considering the current regulatory setting in Canada. A legal expert described how AML legislations and KYC rules are problematic and made online identification almost impossible:

> *"[…] there has been a lot of pressure because of the fact that KYC has been extremely difficult. We're still years away from having a smooth digital ID in Canada."*

It goes without saying, that digital-identity services are really important in the context of open banking and can really boost the customer experience and convenience if the market gets it right. It is also one of the services that can keep the incumbent financial institutions relevant in the long term as it plays to their strengths in terms of their extensive customer base and trusted profile. This is one of the main reasons they have been pro-active in investing and rolling out similar products. Such implementations are definitely moving in the right direction and should be promoted further. Having said that, it's the government's role (through an open banking regulatory framework) to make sure a possible digital identity infrastructure is fair and accessible by all players in order to encourage innovation in this space.

API adoption and standards

Perhaps one of the most important elements for an open banking framework is the design and development of open and common standards for the creation of APIs that will allow ecosystem participants (ASPSPs and TPPs, etc.) to share the required data (e.g. bank account information, transactional and historical account data, payment instructions, etc.) in a uniform way that is understood by all parties. API standards provide the specifications or the "formula" (e.g. architecture, format, documentation, versioning, etc.) that informs the design, development and maintenance of APIs. In that context, open API standards can be created either by one or a consortium of private organizations (i.e. industry-led standards) or an independent entity with that particular mandate (i.e. like in the case of OBIE in the UK Open Banking).

Having a standardized API makes a lot of economic sense as it allows TPPs to connect seamlessly with deposit-taking institutions without making a huge effort to develop new interfaces each time. This kind of smooth integration is a key driver for the development of innovation ecosystems and can play an important role for the development of new business models in banking and finance, more generally, as the industry is becoming more "modular" due to the openness of data and interconnectivity of actors.

The majority of our various stakeholders interviewed acknowledged the importance of APIs in the context of open banking in order to create better connectivity and try to embed financial services across the sector as well as in economic transactions in other industries (a trend also known as 'embedded finance'). A senior figure from one of the large incumbent banks said:

> *"the technology [APIs] enables new use cases and opens this wider for the customers."*

and a FinTech representative confirmed:

> *"If you talk now increasingly to institutional partners who are keen to draw on ventures and joint partnerships, they all acknowledge that the promise of APIs is to build an ecosystem where firms can securely and reliably exchange data using common standards and do this in the direction* [i.e. for the benefit] *of the client. For us this is an obvious and needed thing to scope out what we may build, where should we partner with a third party, and all the thinking around giving the client better access to better products and services."*

Many held a strong conviction that open APIs will facilitate further competition and deliver a more level-playing field for the smaller FinTechs and challenger banks to compete. A challenger bank official argued:

> *"We are building a digital stack with a mind to the open banking world, so we are assuming that there will be a bunch of APIs that will allow us to* […] *have a dashboard that will be provided by us or by somebody else saying 'you get a 0.5%* [interest] *on this deposit, and it has been sitting there for three month and you've been wasting money so why don't you move it across to somewhere else where you can get a higher yield' and that should flatten the funding costs disadvantage we have over the big banks."*

The role of API standards was also emphasised, especially by FinTechs who are seeking better, quicker and less expensive connectivity with bigger players. A FinTech CEO discussed having a universal financial API standard:

> *"That would be awesome to be honest. For us it's a dream to yet be realised because nobody is moving forward at the moment and for now it's only discussions.* […] *we really want to be involved in the potential standards that could be discussed for accessing financial data."*

However, some key Canadian ecosystem FinTech firms were quite sceptical and largely unconvinced that incumbents will have the incentive or the capacity to provide standardised API connectivity to smaller players. They stressed issues around system resilience and uptime performance, as well as the quality of data shared. A FinTech representative illustrated these issues:

> *"We'd love to work with direct APIs but* […] *are we going to get the information that our clients want? Are we going to get them all the time? Because it's a critical service to provide financial data. If you were to connect your bank account and it wouldn't work how likely are you to go back every day to try and connect your bank account? You would likely find another way to transfer your funds".*

Such issues are not pure speculation and have been experienced in the context of open banking in the UK and elsewhere. In general, incumbent banking institutions are slower to transform, less agile, and struggle with costly legacy systems and processes that are hard to

modernise and digitize. Indeed, a Canadian incumbent bank representative, who spoke confidentially, painted a similar picture:

> *"You need to keep the lights on the legacy that we've always done business, because, we can't not do it. And then* [in addition to that]*, we need to invest to create new and enhanced services as well. So, APIs to us is yet another new layer when we can't get rid of the old staff."*

Security, security, security

Unavoidably, any discussion around open banking brings forward issues around the security of the data, both during storage (at the premises of an FI or on the cloud) and whilst being communicated among entities in the open banking universe. When it comes to data-sharing, APIs are deemed as one of the most secure and simplified ways to share data between systems and applications. In addition to the API standards discussed above, security standards that provide a systematic mechanism for accessing the underlying data will create trust in the system and reduce frictions. These involve authorisation and authentication standards as well as standardised permission frameworks. As discussed above, a key debate surrounding security issues in the open banking ecosystem has been the use of alternative data-sharing technologies such as screen-scraping and whether such "older" practices should be applicable and allowed in modern open banking systems.

The big difference between APIs and screen-scraping is that the latter is not permission-based and thus it does not let the end customer control the degree and duration of the access they allow to third-parties (be it data aggregators or FinTechs that do account aggregation). This potentially creates problems as it can compromise protection of the account (e.g. credentials leaked or fraudulent use by rogue agent within the TPP) and also can be a violation of the terms and conditions of the account use asserted by the bank. A technologist and consultant asked about the API vs. screen-scraping debate described:

> *"arguably neither the bank nor the customer that's providing the credentials is on-side of their own terms of use of the agreement when you are providing those credentials to the aggregators* […] *it's inaccurate, it is risky and it creates a bit chaos. The only person who wins in that scenario is the aggregator who can sell* [the data] *– in the short term.* […] *I think open banking creates an opportunity for all parties concerned to legitimise these structures through APIs as opposed to screen-scraping that way credentials are not any longer used and using tokens that sit within the confines of the API-sharing system. It addresses that risk and I think that part increases the impetus to do collaborations and cleanse that data aggregation and screen-scraping approach so that everybody is more on-side."*

Banks generally do not approve of the screen-scraping process to access their customers' financial data but there is little they can do about it:

> *"They are aware of the fact that is happening and they can't prevent their clients from providing credentials."*

Perhaps the most effective way to avoid having their online banking portals web-scraped would be for banks to issue comprehensive APIs, but, for many of the reasons we discussed above, this hasn't been the norm yet. A FinTech founder said:

> *"Banks are trying to push screen-scraping companies as being stealers and people that you should not trust, but the truth is that many screen-scrapers want to use bank APIs. We'd be the first ones to use bank APIs if they were available. But the truth is that when we sit down with incumbent banks in Canada and we tell them that we*

want to use their APIs there is no response from their side. They don't want to solve the problem that their clients are asking for their data."

The prohibition (or not) of screen-scraping in banking is a decision that carries lots of political, economic, and technical weight and can't be taken lightly. As expected, banning screen-scraping would give incumbent banks more control over how and what data they share with thirdparties and it will force the industry periphery to play according to their own terms. At the same time, security concerns cannot be ignored and regulators will have to act in order to protect consumers as they transact in the digital economy. While 'to screen-scrape or not to screen-scrape' is an important live debate and a key concern for various data-sharing frameworks, it's not the only one. A legal expert mentioned:

"There is something to be said about the increase of risk as a result of open banking arrangement, because what happens is that data is seen as currency these days, and so there is going to be a lot more data, and a lot better data, and it's going to be one fat juicy target."

The above view highlights the role of cybersecurity in the context of open banking. However, open banking can also facilitate solutions that will battle such occasions and potentially lead to a safer banking system. A FinTech founder and CEO discussed:

"We had two major security breaches with the Canadian banks last year – what I would expect to happen with open banking […] *is the availability of this dataset through a governing body which would allow specific people to get access to that dataset, and you would have security and specialization firms which look for anomalies within your data to actually better secure you than the existing provisions. So, I think that there are probably some short-term cyber risks but in the long term we're going to be more secure with a data-sharing framework."*

Generally speaking, FinTechs and smaller institutions with smaller budgets and less experience, are often seen as the weakest links in the data-sharing ecosystem and are often asked to increase their security standards and protocols. In the past this has led to disproportionate expectations from FinTechs compared to what the incumbent banks are required to do or used to doing. One of the expert consultants in the sample said:

"You talk to people in the FinTech side and they sort of suggest that they have far better security than the banks do. In the Canadian context for instance, when you take internet banking, none of the big banks here are required to have two-factor authentication for accessing internet banking so [FinTech practitioners would say] *'how can you tell us that we do not know anything about security'? That's sort of the view."*

As expected, there is often a deficit of trust towards newer, smaller, and less reputable organizations. Many of the above debates may bias consumers' perceptions about the validity of third-party services as well as the benefits and safety of open banking solutions as a whole. A technology expert discussed:

"It's a bit ironic. Government says 'the people want this', and then you have people saying 'I don't trust open banking because I don't know what's happening with my data'. Even though there's never been an issue with data in open banking, they just associate it as a risk: 'I want the bank to protect me', or 'I want someone big and strong to protect me', but that's not even a valid conclusion. When you see choice, it's like any uptake of technology. Over time there will be more and more of an uptake from in-person (i.e. bricks-and-mortar) to online channels – it's inevitable".

Data standards

The role financial data standards play in data-sharing is unparalleled. Data standards provide the rules and specifications according to which data are represented, formatted, defined and structured. They allow for a consistent way to describe and record information so that it can be communicated and processed automatically. Data standards in finance are not new. In the past half a century, there have been numerous standardization efforts to provide sets of rules and formats for the exchange of messages between financial institutions for a sizable range of transactions in the payments, banking, and financial markets businesses. These included financial messaging standards for customer payments & cheques, financial institution transfers, collection and cash letters, credits and guarantees, pre-trade, trade, and post-trade instructions, etc. Proprietary standards from individual banks or collective (but often exclusive) efforts such as SWIFT message types and the FIX-protocol gradually gave way to open data standards and the creation of ISO-led unified durable standard schemes, such as ISO20022 which was created to provide interoperability across the entire finance supply chain and service many industry sub-sectors[25] (Scott and Zachariadis, 2014).

As open banking and data-sharing in finance is gaining momentum across the globe, industry participants and regulators realise the importance of commonly accepted data standards. As it stands, the EBA Regulatory Technical Standards (RTS) which are key to achieving the PSD2 regulatory objectives, require that designed APIs "shall use ISO 20022 elements, components or approved message definitions"[26]. To conform with this direction, all “API payloads” are designed and structured around the ISO 20022 message elements and components where possible. Overall, ISO 20022 promotes interoperability between parties during the payments process and allows users and corresponding systems to communicate using consistent language and formatting.

In the context of our Canadian open banking study, there was very limited discussion around data standards and ISO 20022. Having said that, Payments Canada has been actively promoting the adoption and use of ISO 20022 across all its modernization projects, and in the context of Canadian payments between vendors and businesses. The adoption of the UNIFI payment message standard will allow electronic payments to transmit richer data which may lead to further innovation in products and services as well as smoother, faster and more automated payments (Straight Through Processing). In the following section we discuss in more detail how developments around the Canadian payment system may relate to the implementation of open banking.

---

[25] ISO20022, also known as UNIversal Financial Industry (UNIFI) message scheme, is a “standard for standards” which defines the guidelines for the development of individual financial messages. It pulls together three distinctive layers necessary for the creation of standards: the *business process and concepts* that provide all the definitions for the processes and roles of actors, the *logical message* layer which includes all the information needed for the execution of a particular function, and the *syntax* layer that decides on the “physical representation” of the message itself using XML as the principal language. For a detailed discussion of financial messaging standards see Chapter 3 in Scott and Zachariadis (2014).

[26] See the following link for a detailed set of API specifications as part of the PSD2 and UK Open Banking regimes: https://openbanking.atlassian.net/wiki/spaces/DZ/pages/1077805207/Read+Write+Data+API+Specification+-+v3.1.2

Participant goals and concerns

Identification of TTPs

Unavoidably, issues around the previously discussed liability raise questions around the identification of actors in this role-based open data ecosystem. Only providing data access to regulated parties requires the establishment of a company registry or central directory that will identify actors and hold information on their credentials and status. Being on that regulated list will allow parties to claim access to the data. If for any reason any company on the registry is in violation of any of the covenants under which they were granted permission to be on the market, they can simply be 'unplugged' from the market by removing their directory permission until they fix the problem which breaches the terms. In the United Kingdom, the above directory database is being handled and maintained by OBIE. Account providers such as banks, building societies, and payment companies are then enabled to verify the identity of regulated TPPs. Unfortunately, this approach has not been implemented systematically across the EU and there's a current gap that the private sector, through FinTech companies, is trying to fill. Building Identification Infrastructures can also be quite challenging especially in keeping up with data quality issues, but is really pivotal to the functioning of the framework and managing risks (Millo, Panourgias, & Zachariadis, 2019).

Legal experts, in our sample, argued that the Canadian regulatory setting more closely resembles the EU (or the US) system which is a federated economy and certain rules and regulations would apply only at the provincial level. An incumbent bank senior official commented:

> *"If you look at the UK open banking implementation, banks are opening up to FinTechs that have gone through a stringent process and being registered. In Canada, the government would not be able to register everyone to participate in this way. They won't be able to do it for institutions* [like FinTechs] *registered at the provincial level."*

Such issues and conflicts between the federal and the provincial authorities have also occurred in the past. Another large bank manager gave an example:

> *"just like we had payday loans for 20 years and everyone has been moaning about it. They are provincially regulated, the federal government couldn't do a thing about it – they are charging usury rates"*.

Payment systems

Seen as complementary to the open banking efforts, certain data-sharing frameworks (e.g. in countries such as the UK and Australia) are happening in parallel to payment system modernizations that seek to offer banking and non-banking institutions better access to economy-wide payment infrastructures. In Australia, this was explicitly articulated in the findings from the public consultation on open banking that concluded in December 2017. This described the importance of New Payment Platform's (NPP) plans to "enable real time person-to-person payments in addition to more data being able to be included in payment information", especially due to the lack of write-access for payment initiation (Australian Government, 2017). In open banking frameworks where payment initiation is excluded this is ever more important in order to facilitate third-party payment solutions.

In-line with the above developments in the UK and Australia, Payments Canada is currently undergoing a substantial modernization program that seeks to transform the national payment system and prepare it for the next generation of new technologies and consumer demands. The program runs across most payment schemes of the national payment system including its

RTGS system for high-value payments (also known as 'Lynx') and the Automated Clearing and Settlement System (ACSS) for batch payments. It will also introduce a new Real-Time rail that will settle transfer of funds between accounts instantly and act as a platform for innovation.

In spite of the ambitious plans to modernize Canada's payment systems, the current state of the payments landscape has been characterized as slow and inflexible. A banker explained:

> *"it's quite hard to actually move funds around the payments system. The lags are unacceptably large right now but this will change over the next couple of years."*

Another FinTech representative shared similar views by discussing the direct debit business setting:

> "[…] *is a very oligopolistic system in Canada. We were trying to offer* [a service] *currently that's against the 'constitution' of Interac which is owned by the banks so we were unable to crack that. These are the kinds of things that open banking will hopefully enable, there are all sort of kinds of resistance points."*

Interac operates Canada's real-time domestic debit network – a cooperative solution owned by the banks that allows consumers (using their plastic cards and applying their PIN) to transact with their banks' accounts and settle directly with merchants' bank accounts. This current ownership structure makes it difficult for FinTechs and NeoBanks to access this payment system which is quite an essential part of many payment services. When speaking about the payments setting in Canada, a payments expert reinforced the above argument:

> *"The picture I am trying to paint here, is that, those five* [meaning the big five incumbent banks in Canada], *control the landscape."*

Such pain-points are evident in many examples given by the non-bank institutions we talked to. Another interviewee described his frustration with the current system:

> *"we clear through a big bank which takes us longer. We send them a file and they send that file across the banking system and comes down to the other side, so, that's why it takes as long as it does to move money across the banking system. But when the real time rail comes with Payments Canada's payment modernization hopefully we'll be able to face the system directly and have real-time money movement* […] *the challenge is that the real-time rail itself is a couple of years away at least."*

Such issues could be resolved both through the payment systems modernization as the new scheme will, hopefully, provide greater access to smaller, non-bank institutions and help them compete in the market on an equal basis; as well as an open banking framework that includes a payment initiation functionality. A FinTech startup senior employee explained the company's position:

> *"[…] typically open banking and payments are part of the two sides of the same coin. […] we are directly interested in better payments landscapes and technology in Canada. And that is like core of the product experience – there is a lot of payments experience in the customer banking infrastructure in Canada. And so open banking being part of that thing which accelerates payments and facilitates payments* […] *it's very interesting to us."*

The findings also suggest that there is a need to harmonize any open banking directive with existing developments in payments so that issues are being addressed collectively for a better industry outcome. This, of course, applies across all aspects of data-sharing in banking (e.g.

data privacy, security, digital identity, standards, technology, etc.) but is particularly important for payments as they are central to any economic transaction.

> *"The alternative and probably the better alternative from our perspective would be updating the consumer right as well as creating a unified standard and a registration around AISPs like in the UK, ensuring that it ties into the payments modernization act and the role of PSPs, because if you have open banking without payment initiation services there's a half-baked solution."*

Impact of open banking on the market structure and business models

How is open banking going to affect competition in the sector, and what will it do to business models? While this discussion goes beyond the objectives and findings of this paper[27], it would be useful to provide a short review of the existing literature and discuss potential effects of data-sharing frameworks for the industry.

It is profound that open banking can have a significant impact on how competitive dynamics are formed in the financial services sector as well as on the business models of incumbent banks, FinTechs, and other well-established intermediaries and infrastructures within the finance industry. Zachariadis and Ozcan (2017) deliver an in-depth discussion on how an open API economy in finance can provide solid ground for the emergence of platforms and FinTech ecosystems around them. Platforms can be conceived as multi-sided networks that capitalise on transaction cost economics and network externalities to profit from the facilitation of interactions when market or hierarchy alternatives are more expensive - often due to high costs of contracting or acquisition (Zachariadis et al., 2018). In the era of open data in banking, this could be a useful approach to explore (particularly for incumbent of challenger banks) as they can become mediators of economic activity and sit in the middle of interactions between FinTechs (TPPs) and the end customers. This means that bank profits in the future could come from selling technology or access to TPPs to an organised electronic marketplace (where they can sell their products to the bank's customers) rather than selling traditional banking services to their clients. This should allow them to (re-)sell more innovative services to their customers (even though they did not "produce" them) and keep them engaged on their own platform reaping the benefits from data monetisation. While the above scenario sounds quite luring and could potentially provide an opportunity for the banks to lead the way in terms of new business models, research shows that they are facing multiple issues that relate to their legacy systems, institutional logics, organizational culture, collaborative appetite, etc. (Ozcan, Zachariadis, & Dinckol, 2019).

In the above context, and as finance is becoming more and more embedded in economic activities across various industries, digital IDs can be an effective vehicle for large banks to leverage their strengths and establish themselves as focal points for any financial transaction consumers will want to pursue. With greater use of technology and greater circulation of data

[27] During the initial set of pilot interviews, research participants were asked about the impact of open banking on the competitiveness of the incumbent banks and FinTech companies. As the discussion around open banking in Canada was in the earliest of stages, there was virtually very little information around the nature or type of open banking implementation the government would pursue. As a result, the majority of participants were hesitant to give answers to such questions and hard for this study to draw any meaningful conclusions around open banking strategies.

in the financial system, comes greater challenges around privacy and security. Large deposit-taking institutions are currently trusted with customers' identification and reference data (e.g. customer IDs, proof of address, etc.). Thus, they could capitalise on that and safeguard customers' identity when they transact through digital channels (Zachariadis, 2019). This, however, would require them to build further on their existing infrastructure and take advantage of new authentication protocols and communication standards to interface with external marketplaces or platforms. In his book "Identity is the new money", Birch (2014) discusses how the convergence of identity and money has accelerated with the extensive influence of social media and mobile phones, leading us to rethink identity in the digital age. To that end, managing people's privacy and confirming their identity online will be vital benefits. This will give choice to consumers when they want to share some of their credentials but remain anonymous to certain providers or networks (Zachariadis, 2019).

Alternative business models have been documented in the practitioners' literature. For example, certain banks may choose to function more as infrastructure or back-office providers, leaving the distribution of their products to FinTechs and other third-parties that specialise in better user experience on a digital or mobile channel (e.g. account aggregators and personal finance management apps). This is a legitimate business which, under certain circumstances and market conditions, can be very profitable. Such a model, often referred to as "banking-as-a-service" (BaaS) would normally require investment in digital transformation to enhance the core infrastructure and make it cheaper to run but while building good connectivity to services and systems. It would also require change in mentality as banks' customers would then be other banks (more likely smaller digital NeoBanks) who want to build on top of an existing infrastructure rather than build their own. Some examples of pure-play BaaS providers in Europe are Solaris Bank and ClearBank. There are also BaaS firms that operate as a regular bank, i.e. providing retail banking solutions (e.g. Starling Bank, Fidor Banks, etc.).

Depending on the level of openness, service distribution, and product creation, one can improvise different business models and make strategic choices about how they wish to compete in the industry as it becomes more digitized and digitalized (ABE-EBA, 2016). On that note, some banks may wish to adopt a hybrid approach that builds both on existing infrastructure and distribution of own products (i.e. integrated "pipeline" arrangement) as well as a marketplace that will channel third-party solutions to customers. One can take as example similar implementations in tech platforms such as Amazon or iOS where both firms' products or mobile apps as well as external merchants' or developers' are being traded. The spectrum of business models from fully-integrated, to producer, BaaS, distributor, and/or bank-as-a-platform is still not fully understood, and many financial institutions experiment with the various options and the impact these may have on their bottom-line performance.

Looking forward to the imminent growth of the API economy in finance, a key feature for the deployment of many of the above business models (especially in the context of platforms) is the investment in, and voluntary creation of, premium APIs that will go above and beyond the mandated interfaces and provide increased functionality to third-parties. These should offer a profitmaking incentive for banks to grow their open banking ecosystem. Such an approach is subject to successful collaborations that the banks will need to strike - thus changing their mindsets and starting to look at TPPs more as their clients and less as their competitors.

Generally speaking, future business model formation by FinTechs, challenger banks, and incumbents in Canada will largely depend on the regulatory setting and impending open banking implementation. It remains to be seen what the future holds for the Canadian banking system and what appetite there will be from both the industry as well as consumers prepared to adopt and use open banking services.

References

ABE-EBA (2016). "Understanding the business relevance of Open APIs and Open Banking for banks", European Banking Association Working Group on Electronic Alternative Payments, Information Paper, Version 1.0.

Australian Government (2017). "Review into Open Banking: Giving customers, choice, convenience, and confidence", Australian Government, The Treasury.

Australian Government (2018). "Consumer Data Right", Australian Government, The Treasury.

Bátiz-Lazo, B., & Wood, D. (2002). "An historical appraisal of information technology in commercial banking", *Electronic Markets*, 12, 192–205.

Bernardo Bátiz-Lazo, J. Carles Maixé-Altés, and Paul Thomes. (2011). *Technological Innovation in Retail Finance: International Historical Perspectives* (New York, NY: Routledge).

Birch, David (2014). *Identity is the New Money*, London: London Publishing Partnerships.

CMA (2016). "Retail banking market investigation – Final report", Competition & Markets Authority.

CMA (2017). "The Retail Banking Market Investigation Order 2017", Competition & Markets Authority.

Department of Finance Canada (2020). "Consumer-directed finance: the future of financial services", Accessed here: https://www.canada.ca/en/department-finance/programs/consultations/2019/open-banking/report.html

Fingleton Associates (2014). "Data Sharing and Open Data for Banks", Report for HM Treasury and Cabinet Office.

Fingleton (2019). "Open Banking, Preparing for lift off" Fingleton and Open Data Institute, June 2019.

Ghazawneh, A. and Henfridsson, O. (2013). "Balancing platform control and external contribution in third-party development: the boundary resources model", *Information Systems Journal*, Volume 23, Number 2, 173-192.

Iacovou, C., Benbasat, I., & Dexter, A. (1995). "Electronic Data Interchange and Small Organizations: Adoption and Impact of Technology", *MIS Quarterly, 19*(4), 465-485. doi:10.2307/249629

Jacobson, D., Brail, G., & Woods, D. (2012). *APIs: A Strategy Guide* (O'Reilly).

Layder, D. (1990). The Realist Image in Social Science, New York: St. Martin's Press, pp. 1-189.

ODI (2016). “Introducing the Open Banking standard”, Open Data Institute, ODI-WP-2016-001.

Mazer, Rafe (2018). “Emerging Data Sharing Models to Promote Financial Service Innovation: Global trends and their implications for emerging markets”, independent report supported by The Bill & Melinda Gates Foundation.

Millo, Y., Panourgias N.S., Zachariadis, M. (2019). "Capitalization by certification: creating information-based assets through the establishment of an identification infrastructure" in Kornberger M., Bowker, G., Pollock, N., Miller, P., Mennicken, A., Elyacha, J. (eds) *Thinking Infrastructures*, Emerald Publishing.

Ozcan, P., Zachariadis, M., & Dinckol, D. (2019). “Platformification of Banking: Strategy and challenges of challenger versus incumbent banks in UK", Proceedings of the *79th Annual Meeting of the Academy of Management*, 9-13 August, Boston, Massachusetts.

Payments Forum UK (2015). “The Open Banking Standard – Unlocking the potential of open banking to improve competition, efficiency and stimulate innovation”.

Sayer, A. (2000). *Realism and Social Science*, London: Sage Publications, pp. 1-301.

Scott, S. V. and Zachariadis, M. (2012). "Origins and development of SWIFT, 1973–2009", *Business History*, Volume 54, Number 3, 462-482.

Scott, S.V. and Zachariadis, M. (2014). *The Society for Worldwide Interbank Financial Telecommunication (SWIFT): Cooperative governance for network innovation, standards, and community*. London: Routledge (Global Institutions Series). ISBN-10: 0415631645 | ISBN-13: 978-0415631648.

Tilson D. Lyytinen K. Sørensen C. (2010). “Research commentary—Digital infrastructures: The missing IS research agenda”, *Information Systems Research*, 21(4), 748–759. 10.1287/isre.1100.0318.

Tsoukas, H. (1989). “The Validity of Idiographic Research Explanations,” *Academy of Management Review* (14:4), pp. 551-561.

Volkoff, O., Strong, D. M., and Elmes, M. B. (2007). “Technological Embeddedness and Organizational Change,” *Organization Science* (18:5), pp. 832-848.

Zachariadis, Markos. (2019). “Banking of the Future: Finance in the Digital Age”, HSBC Report.

Zachariadis, M. and Ozcan, P. (2017). “The API Economy and Digital Transformation in Financial Services: The Case of Open Banking”, *SWIFT Institute Working Paper* No. 2016-001.

Zachariadis, M., Ozcan, P., & Dinckol, D. (2018). “The Economics and Strategy of Platforms: Competing in the Era of Open Banking” in Maslaveckas, Ed (eds) *The Book on Open Banking: A Series of Essays on the next Evolution of Money*, Bud Financial Limited.