CCUA
Canadian Credit Union Association

ACCF
Association canadienne des coopératives financières

# The Merits of Open Banking – CCUA Submission

Submitted on:

2019-02-11

Canadian Credit Union Association
Association canadienne des coopératives financières

151 Yonge Street / rue Yonge
Suite 1000 / bureau 1000
Toronto, ON M5C 2W7
Tel: / Tél. : 416.232.3422
Fax: / Téléc : 416.797.0563

ccua.com

# Table of Contents

# Introduction

The Canadian Credit Union Association (CCUA) welcomes the opportunity to participate in the Department of Finance's consultation on the merits of open banking in the Canadian financial services sector.

The CCUA endorses the aims of the Department of Finance in examining the merits of Open Banking. Open Banking, if implemented correctly, has the potential to bring further innovation into the Canadian financial sector to the benefit of Canadian citizens, as well as make Canada more competitive internationally.

As the Department of Finance has recognized, the introduction of Open Banking in Canada must be implemented in a way that ensures the safety and soundness of the existing, trusted financial sector in Canada. The following paper presents our sectors views on the potential implementation of an Open Banking model in Canada.

# General Comments

Credit unions are financial co-operatives, meaning that they are democratically controlled, member-owned organizations that follow a set of ethical principles when making business decisions.[1] They have operated in Canada for over 100 years, and are trusted institutions in communities across Canada. This trust comes from the knowledge our members have that their credit union is a secure, stable, and transparent financial institution that treats their personal information with the utmost care.

As member-owned financial institutions, Canada's credit unions exist to serve the best interests of their members. Canadian credit unions are developing a self-imposed Market Conduct Code, due for adoption at the end of 2019. In this Code of Conduct, credit unions are codifying our industry-leading best practices as protectors of their members' personal private information, while remaining in compliance with the Personal Information Protection and Electronic Documents Act (PIPEDA) and provincial privacy legislation, where applicable.

Credit unions have always seen themselves as stewards of members' financial data, not owners, and this frames our perspective on the concept of Open Banking. The implementation of Open Banking, if such a framework were to be introduced in Canada, should be to benefit our members. This commitment to credit union members takes priority over other objectives of this framework, such as global competitiveness.

There are several initiatives underway in Canada that are and will be affecting Canadian financial institutions over the next few years. Payments modernization and the increasing use of digital identification will change the way Canadians interact with their financial institutions and other sectors. Not all these initiatives can be done concurrently if Canadians' data security is to be maintained. As we will detail, privacy and security

[1] https://www.ica.coop/en/cooperatives/cooperative-identity

concerns should first be addressed by the government before the implementation of an Open Banking framework. This includes a modernization of PIPEDA and the implementation of a national digital ID system. These are foundational features of a secure Open Banking ecosystem. Payments modernization is already underway and will have an impact on the type of services offered by financial institutions.

CCUA recognizes that the Finance Department's consultation document on Open Banking are concerned with the merits of such a system. However, after consultation with our member credit unions, colleagues in Europe, privacy experts, and compliance professionals, several issues of significance have been raised that have caused some reluctance and concern. We will address these issues in this submission.

It should be noted that organizationally the CCUA represents 250 credit unions that are diverse in size, geography, technological capacity, and opinion. While this submission reflects risks that members have raised, it is worth noting that credit unions have indicated they are optimistic about the opportunities that Open Banking will create.

Overall, Canadian credit unions are supportive of the introduction of an Open Banking regulatory framework. Credit unions are optimistic that with prudent implementation and ongoing meaningful consultation, Open Banking will benefit their members and Canada as a whole.

# The Merits of Open Banking

> *Would open banking provide meaningful benefits to and improve outcomes for Canadians? In what ways?*

An Open Banking framework would solve several significant problems facing the financial services sector in Canada. We explore these opportunities below under the headings of modernization, competition, and digitization.

## Modernization

Many financial institutions in Canada are using "legacy" systems to perform day to day banking operations. While these systems are effective, they can impede innovation in financial service offerings, owing to their complexity and the high capital cost to operate. Further, many of these legacy systems are in place to maintain compliance with the increasingly complex regulatory system that all financial institutions, including credit unions, must adhere to. CCUA considers that the introduction of an Open Banking regulatory framework could have the positive down-stream effect of modernizing some of the existing rules and regulations that credit unions must comply with, thereby allowing them to operate more cohesively and efficiently. For credit unions, the cost to comply with the various regulations that exist at all levels in Canada is much higher, proportionally, than the large banks. Anything to bring down this relatively much higher cost would be good for our members and for competition in financial services in Canada, which is currently suboptimal.

The introduction of Open Banking will provide more data access to the financial services provider hosting it. This should result in the increased use of data analytics, machine learning, and other data concepts to enable new and better processes and services. Open Banking should also strengthen data-based decision making at financial institutions, leading to more innovative and customized services for Canadian consumers.

Credit union members, like all Canadians, want more convenient and faster access to financial services. CCUA sees an Open Banking framework as a means to increase the convenience and ease of day-to-day financial transactions and provide members with a more complete, holistic, and personal, financial picture. Likewise, for Small and Medium Enterprises (SMEs), Open Banking should provide them with a more holistic and convenient way to view their finances, allowing them to focus time on their business operations.

## Competition

A well-designed Open Banking framework will give space for smaller financial institutions like credit unions, and fintechs, to compete. Credit unions pride themselves as being leaders in member/client service. This is rooted in their co-operative governing principles and organizational structure. Open Banking could increase Canadians' awareness of the credit union alternative.

Such a framework could increase the diversity of competition in financial services and allow consumers to make more rational market-based decisions. With this increased competition, and the concept of financial data portability, transferring between financial institutions could become easier. While concerns exist around how certain features such as account switching will be implemented, credit unions see the advent of Open Banking as a positive development to increase fair competition in the financial services sector in Canada.

Creating a single, standard, open Application Programming Interface (API) will also lead to increased competition. Rather than having to develop for multiple APIs (with different data definitions and data mapping exercises, security requirements, etc.) that financial service providers want to connect to, financial institutions and fintechs will be able to work on the same specifications. This could result in the faster integration of new technologies, quicker introduction of new innovations, and a more level playing field.

## Digitization and Digital ID

Data sharing between financial services providers will lead to the further digitization of many financial transactions. This digitization has the potential to save consumers time and provide more convenience for consumers who are unable to access a physical branch.[2]

---

[2] It should be noted that many rural areas in Canada still have trouble accessing high speed internet.

In order for the digitization of these services and processes to be implemented, changes in regulation, both provincially and nationally, are required to allow for the acceptance of digital signatures or Digital ID.[3] In a Digital ID plus Open Banking environment, there will be less opportunity for physical identity fraud and data mismatches (such as individuals with the same name creating erroneous transactions), while credential authentication will be more efficient. A Digital ID plus Open Banking system will allow for data portability, with data ownership being put into the hands of the consumer, as opposed to the organizations with whom they do business.

CCUA and many Canadian credit unions participate in the Digital Identity and Authentication Council of Canada (DIACC), a national association with members in both government and the private sector whose aim is to introduce a national digital identification and authentication framework in Canada. The credit union sector is currently contributing to a white paper on the importance of Digital ID to an Open Banking framework.

Open Banking should be introduced in lockstep with or after the implementation of a cross-sectoral Digital ID system. Doing so will increase trust and better socialize and expose Open Banking to Canadians. It will also provide Canadians with a simpler understanding of consent and their personal data rights, as opposed to understanding Open Banking data rights and Digital ID data rights independently of each other.

## Addressing Risks

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

It is imperative that any regulations governing Open Banking have a strong consumer protection orientation. Consumer protection should be the main priority of any Open Banking framework, overriding all other concerns. Specifically, the Open Banking framework should include rules that protect the most financially vulnerable and technologically-adverse consumers. To mitigate the risk of financial exploitation by aggressive financial services providers, a strict consumer-centric regulatory regime is required to ensure trust in the Open Banking environment.

Further, as one of the largest lenders to Canadian Small and Medium Enterprises (SMEs), credit unions believe that the introduction of Open Banking should also include strong protection for SMEs.

---

[3] As well as the socialization of Digital ID.

## Consumer Protection

> *This consultation paper seeks views on what specific consumer protection elements are needed for the sharing of financial transaction data under Open Banking.*

Open Banking has to be built on a foundation of consumer protection that minimizes the threat of exploitation and creates strong requirements to protect consumers.

A strong enforced certification process must be required for all participants in the Open Banking ecosystem. Credit unions want to ensure that their members' privacy and data is protected. With recent events regarding cyber security data issues, credit unions are concerned with sharing their member's data with other organizations if they are not compliant with the same high data protection standards that they follow. This certification should also require that all FSP participants have consumer protection rules in place, such as the credit union's Market Conduct Code.[4]

CCUA is ready and willing to provide input to Government to help design an industry-wide process that will enable consumers to challenge FIs when there has been a failure in the system (such as a data breach or fraudulent activity). Furthermore, mechanisms should be in place to ensure that consumers are aware of their rights if there is a failure or fraudulent activity with one of the financial service providers they are using.

Within the consultation, one of the benefits of Open Banking is "the ability for consumers to input information about their financial history to *receive offers for financial products that are personalized and targeted to their financial needs*" (emphasis added). This statement, and other aspects of Open Banking, raise consumer protection concerns such as:

- Consumers should be provided with appropriate and clear product information (Fair Sales)
- To ensure compliance with fair sales practices, offers to consumers should be appropriate and drafted in clear language. Direction may be needed on the required language in these offers.
- The information provided to consumers regarding financial products and services should be presented in a manner that allows the consumer to be properly informed and make enlightened decisions. The scope of the information provided should be dependent on the type and complexity of the product
- Financial Service Providers (FSPs) must not knowingly take advantage of a consumer who is unable to protect their own interests. If a vulnerable consumer receives several product offers from several FSPs and subsequently acquires all of the products, the consumer could be placed in a difficult financial situation (e.g. too

[4] https://www.ccua.com/news/2018_09_27_market_code

much debt). FSPs should make product recommendations to consumers that are reflective of the financial needs and circumstances of the consumer.

- Consumers must be made aware that there may be an increased risk of being "spammed" with similar product offerings from several FSPs.

- Further, because Open Banking, and the concept of data portability, is a new concept in Canada it will require strong education and socialization amongst Canadian consumers. Without appropriate education, there is an increased risk of misinformation and fraud. Even the term "Open Banking" is a target for misrepresentation. Most consumers today are unlikely to have an elevated level of awareness of what Open Banking actually means.

## Citizen Privacy and Consent

> *This consultation paper seeks input on managing the risks or enhancing the benefits that Open Banking may pose from a privacy perspective.*

Open Banking increases the potential for Canadians' personally identifiable information (PII) and financial transactional data to be violated. While all violations of a person's privacy are wrong, the violation of someone's financial privacy is particularly hazardous. As such, any Open Banking framework should hold privacy and consent as paramount relative to other aspects of the framework.

CCUA agrees with many of the recommendations in the Information and Communications Technology Council's report on a Data Economy Strategy, which states:

> "Canadians need a national data consent legislative framework to not only protect their rights, but to disambiguate the differences between PIPEDA and provincial privacy regulations – some of which can be challenging to compartmentalize."[5]

Moreover, there are potential risks relating to consumer consent for data sharing. Credit unions recognize that there are ample ways where a consumer, who has a reasonable level of knowledge of digital risk, could be compromised. Open Banking should not increase their burden in receiving financial services, lest the merits of Open Banking be diminished.

In order to mitigate these risks, the recommendations by the Privacy Commissioner's Office on meaningful consent that were released in May 2018 to achieve informed consent should be incorporated into the framework.[6] While more discussion is required around what, where,

---

[5] https://www.ictc-ctic.ca/wp-content/uploads/2018/11/ICTC_Whitepaper_Perspective-Data-Econ-Strat.pdf
[6] https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/

and when specific parts of the guideline are applied, the Privacy Commissioner's recommendations provide a strong foundation to begin creating technical requirements for meaningful/informed consent. Further, "Privacy by Design", a concept introduced by Canadian professor Dr. Ann Cavoukian,[7] are principles that should be considered in the foundation and adoption of any Open Banking framework.

## Liability

In discussions with member credit unions, peer organizations, and other experts, issues around liability and recourse are some of the most common concerns about Open Banking implementation. Many of the concerns raised primarily concern reputational risk and financial risk as they relate to liability in an Open Banking environment.

When considering financial risk, we ask the government to consider: in situations of data breaches where financial transaction data and/or PII is leaked or stolen, which party is financially liable for recourse? A fair system should ensure that it should be the violating party's responsibility to solely cover any financial loss. Further, all participants in an Open Banking ecosystem must have adequate liability insurance coverage to cover potential losses. It may be prudent to have an adjudication body to determine who is liable in these situations to expedite resolution rather than seeking legal recourse through the judicial system.

It is much more difficult to determine who is liable when it comes to reputational risk. In a case where a credit union is the primary financial institution of a member and a security breach may occur to another FI, a member may hold the credit union responsible. This may be due to a lack of understanding regarding the Open Banking system and how it operates. This situation could unfairly tarnish the reputation of a credit union that had no control over the third party's cyber security. We ask the government to consider potential scenarios like this, and other liability issues, when developing the Open Banking framework.

## Financial System Stability

> *This consultation seeks stakeholder perspectives on whether open banking presents new prudential risks to financial institutions, and related mitigants to those risks.*

### Regulatory Burden and Externalized Costs

The development of an Open Banking framework will have to be mindful of the significantly increased expenses that could be imposed on smaller entities to comply with the relevant application program interface (API) standards. As noted earlier, compliance costs tend to land disproportionately on smaller institutions like credit unions and the resulting cost pass-through effects could offset in large measure the credit union system's competitive advantage around member services. High compliance costs would take a larger amount of credit union profit and therefore capital available to invest in new products and services,

[7] https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf

decreasing competition with larger financial institutions. Policymakers must consider the competitive (price-side) impacts of moving to an Open Banking framework for existing small financial institutions.

The increased convenience of account switching, account set up, and complex transactions between financial institutions will undoubtedly lead to an increased volume of these actions occurring. These actions will still require regulatory compliance and due diligence processes such as Know Your Customer (KYC), Anti-Money Laundering (AML), and others. While Digital ID should assist in some of these credential verification issues, credit union staff will still be required to ensure regulatory compliance by reviewing member accounts. The increased transaction volume may lead to higher compliance costs borne by credit unions. The government should consider how the higher volume of transactions that require KYC and AML due diligence will affect credit unions operating costs.

## Technology Cost Considerations

Credit unions operate in a diverse system that includes co-operation between their sister credit unions, and with collectively owned IT organizations to achieve economies of scale, but they also have autonomous and independent decision making around their IT infrastructure. Under an Open Banking framework, credit unions would need to consider the best way to enter this environment. This would require a sufficient notice period to ensure that each credit union is able to participate while ensuring their financial sustainability and maintaining alignment with their organization's IT strategy.

Even the largest financial institutions in Canada do not have the technology in place to accommodate some aspects of what would be required under an Open Banking framework. Digital ID and data portability features are still being developed worldwide and require new software and comprehensive infrastructure changes. The government needs to consider this technology deficit in its implementation timeline.

## Business Model Risks, Branches, and Marginalized Communities

With the introduction of an Open Banking framework, the digitization of financial services will likely accelerate. With fintechs having easier access to client data, direct interactions with financial institutions like credit unions may decrease, while transactions through a fintech's platform may increase. More competition may come from fewer fintechs, that could become the centre of consumer's financial interactions. This could lead to swift disintermediation for existing financial institutions. Banks and Credit unions could become financial services "utilities", whereby their brands and full-service offerings are no longer viable.

The CCUA is concerned that the disintermediation of credit unions could lead to low profitability/branch use, and consequently the closure of credit union branches in small rural communities. Canada's low population density means that initiatives like this create long-term risk to rural Canada as financial institution branches continue to close. When branches close, rural Canadians are often required to then drive hours to the next branch, damaging the local economy.

There are many Canadians who still rely on their credit union's local knowledge and branch support, including residents with limited digital experience and/or a financial literacy deficits. A lack of Open Banking access could create challenges for these people in both rural and urban areas. Open Banking may have the unintended effect of further alienating the unbanked.

We encourage the government to consider the potentially destabilizing impacts of Open Banking on smaller financial institutions and the marginalized communities they serve as it determines timelines and the sequence of implementation.

### Jurisdictional Issues

As most Canadian credit unions are provincially regulated, an Open Banking framework would likely not initially apply to most credit unions. However, in some western provinces for example, the market penetration of credit unions is close to 50% of the population. It is exceptionally important that provincially regulated financial institutions like credit unions be able to voluntarily participate in the Open Banking framework. Cooperation between provincial and national regulators is essential to facilitate this. If credit unions do not have access to Open Banking, they won't be able to provide their members with the same services federal bank customers have access to.

Certain jurisdictional issues will need to be addressed before implementation. For example, consumer protection is under the jurisdiction of provincial governments. If the Open Banking framework mandates consumer protection rules that do not align with provincial consumer protection rules, credit unions may be in conflict with one of the two rule sets.

Additionally, if Open Banking allows for cross-provincial members to use the services of a credit union, this could lead to some credit unions having many members outside of their province of operation. For example, Ontario's Credit Union and Caisses Populaires Act only allows for a maximum of 3% of a credit union's membership to be outside

It is absolutely essential that the government consider these, and other jurisdictional issues, as they develop the open banking framework.

## Technical Standards

While this consultation does not request, or aim to determine, what technical standards should be implemented into an Open Banking regulatory framework in Canada, it is important to raise some concerns around the impending discussion.

### Screen Scraping

The practice of "screen-scraping' in which usernames and passwords are provided to a third-party software to login and pull data from the screen is a practice that should not be permitted in an Open Banking framework. The concentration of user login data under a centralized database outside of financial institutions' control presents an unnecessary security risk. Further, screen scraping can create time delays between the third-party app and the financial institution's database, leading to misinformation and possible erroneous

transactions. We encourage the government to require Open Banking participants to use secure APIs to share data.

## Single, Standard, Open API

A single, open, standardized API represents the best option for an Open Banking framework, to allow a fair and competitive playing field.

As stated previously, the creation of open technical standards should result in an even playing field for all financial services providers. Without it, Open Banking could decrease competition in the sector by giving an advantage to financial institutions with more resources to work with multiple APIs.

- If the API were to be closed or proprietary, there would be fewer eyes on the API code, which could lead to an increased chance that exploits or errors could be made in its development. Further, a proprietary API may require Open Banking participants to pay to access the API, creating a barrier to fintechs and small financial institutions to access and develop innovative technology.

- If there were multiple APIs, developers may end up making their applications compatible with only the most popular API, leaving some financial service providers to either develop their own compatibility, or be left out of the open banking ecosystem.

- If the API is not standardized, there exists the possibility that some APIs would be less secure or have more lenient credential authorization policies. This could create a patchwork of technologies by different FSPs, decreasing compliance and security expectations and minimizing trust in the Open Banking ecosystem.

## Cyber Security

*This consultation paper seeks input on managing the risks or enhancing the benefits that open banking may pose from a cyber security perspective.*

Open Banking will create new cyber security risks, while eliminating old ones. A well-implemented API and Digital ID system would increase privacy and allow for only pertinent information to be shared between financial service providers. However, new vectors of attack will appear when the Open Banking API becomes accessible.

Recent security lapses at financial institutions that resulted in the leaking of personally identifiable information shows that without proper cyber security systems in place, Open Banking could potentially amplify a consumer's financial loss with all of their accounts connected.

Further, with the introduction of quantum encryption (and therefore quantum decryption), researchers at the US National Institute of Standards and Technology (NIST) suggest existing encryption technology could be out of date in less than 15 years.[8]

Given this, and other hard to eliminate cyber security risks (such as phishing and malware), the government should take a categorical look at potential cyber security risks that could occur in an Open Banking system. Government oversight of the technical implementation of the Open Banking API is necessary to ensure that these risks are being mitigated in a reasonable way.

# Implementation

> *If you are of the view that Canada should move forward with implementing an open banking system, what role and steps are appropriate for the federal government to take in the implementation of open banking?*
>
> *[...]*
>
> *While the primary objective of this paper is to facilitate a dialogue to assess the potential merits of open banking in Canada, stakeholder input on implementation considerations that would maximize the potential benefits of open banking and ensure consumer confidence is also welcomed at this time.*

In order to achieve a successful and widely adopted open banking system in Canada, the government should continuously consider the following three areas when making decisions on the design of the framework: Privacy and Consent, Technology and Cyber Security, and Regulatory considerations. These three underlying principles are an important foundation to developing a successful Open Banking framework.

## Consumer Protection and Privacy

### Privacy and Consent

As previously mentioned, focus on privacy and consent are paramount to developing public trust in an Open Banking environment. Part of this requires PIPEDA and potentially provincial privacy legislation to be updated to reflect the modern digital privacy and consent concerns. Any Open Banking framework should be developed in lock-step with federal and provincial privacy legislation to minimize the potential for legal ambiguities or contradictions. If the Open Banking framework is introduced with gaps in requirements around privacy or consent, this could delay the implementation and socialization of Open Banking. Financial institutions should be prepared to work closely with the government and

---

[8] https://csrc.nist.gov/csrc/media/projects/post-quantum-cryptography/documents/pqcrypto-2016-presentation.pdf

data privacy advocacy groups to ensure that any Open Banking framework minimizes potential issues around privacy and consent.

Privacy concepts such as Zero-Knowledge Proof, where only the minimum required information is provided to verify a user, should be considered in the framework. As mentioned, the principles of Privacy by Design, where privacy is embedded at the start and not on an ad-hoc add-on basis, is the credit union's system preference.

### Socialization

Policy and legal frameworks must adjust to manage risks. In parallel, consumers will also need to be well-informed and educated on their rights and responsibilities with respect to data management.

A strong awareness and education campaign during Open Banking's introduction in Canada is required to ensure that consumers know their rights and responsibilities in an Open Banking system. Significant risks for fraud and exploitation of Canadian consumers exists when any new technology is introduced; Open Banking is no different. Canadians must be made aware of what new rights they will receive with regards to the ownership of their data, and what risks they are exposing themselves to if they participate in an Open Banking ecosystem. The proper introduction of the concept of Open Banking to the general public is key to its successful implementation.

Some potential options to socialize Open Banking include public awareness campaigns, incorporating the topic into personal finance education course curriculum, and having a certification seal for trusted open banking participants.

## Regulation

Credit unions are strictly regulated, to the point where the regulatory burden sometimes impedes their ability to innovate. To maintain the competitiveness of credit unions, CCUA stands ready to work with the government to ensure that the Open Banking framework regulatory requirements are manageable for existing credit unions that want to participate.

All participants in the Open Banking ecosystem should be required to meet the same strict requirements around the security, consent, and privacy of client data that credit unions already do. As mentioned, Credit unions do not want to have to spend their time and resources to ensure that that a third party is compliant with those cyber security and privacy/consent requirements. Therefore, Canada's Open Banking framework needs to include strong oversight by the government over all entities authorized to access open banking data. Specifically, a regulatory body should enforce the certification of financial institutions and fintechs that participate in the open banking environment. Routine audits of the security of client data should be required. A formal regulatory authority and structure is necessary to build trust with consumers that their data is secure.

This regulatory body should produce guidelines for participants in the Open Banking ecosystem. It should also develop and manage an Open Banking Directory which displays

regulated participants like banks, credit unions and other third party providers for transparency and public verification. This regulatory body should also be responsible for, or partner with industry-led implementation of a single, standard, open API for Open Banking participation. Payments Canada is a good example of how an API standard could be developed and regulated with government and industry input.

In its implementation the CCUA would also like the ability to comment on regulatory technical standards before they are introduced. One example of this is the European Commission's model of allowing for well-spaced out timelines for commentary on different aspects of their Payment Services Directive 2 consultation. This will allow for industry groups and financial institutions, as well as fintechs, to properly consider the implications of each technical standard and provide reasoned comment to government. Similar approaches would be welcomed by credit unions.

Furthermore, the scope of the Open Banking framework is also critical. Will Open Banking apply to investments, RRSPs, TFSAs, insurance products, mortgages, term deposits, and other financial products? Or will it only apply to chequing and savings accounts, or just chequing accounts? Will all federal financial institutions be required to participate, or only the big banks? Will Open Banking mandate account opening and closing actions, or just allow for the aggregation of data? Will SMEs have access to Open Banking, like individuals? It is clear there are many variations/options to consider, and the government should define what a successful framework implementation will look like.

One potential way forward, could be the creation of an Open Banking Sandbox, where all financial institutions could participate in an Open Banking environment without existing regulatory restrictions around service provision. For example, allowing for clients to view their insurance and chequing accounts on the same interface. Similar examples have been used to success in the broader fintech environment.

Further review and discussion of what systems would be required in an open banking environment will need to be addressed early in the introduction of Open Banking. For example, with regards to rules around how revocation of consent for data sharing with a financial institution will work. Is the requirement immediate, or will the financial institution have a period of time to comply and archive their data for compliance purposes? We encourage the attendance of provincial regulators and OSFI during these discussions.

## Payments Initiation

Credit unions have been monitoring Payments Canada's modernization initiative and their Real Time Rail initiative. The Large Credit Union Council (LCUC) Chief Information Officer group, which represents 16 of the largest credit unions in Canada, have been working together to adopt a unified API standard in anticipation of the Payments Canada modernization and an Open Banking framework. The LCUC and CCUA continue to monitor the development of the Payments Canada modernization.

As such, payments initiation should not be a part of the Open Banking framework in its initial implementation in Canada. Completing the Payments Canada modernization before

any mandated payments initiation in Open Banking would potentially avoid the duplication of costly investment. Moreover, without developing the Payments Canada system first, the risk of multiple standards on payments initiation could occur. We encourage the government to focus on implementing and maturing the foundational elements of Open Banking such as Governance/Oversight, Privacy, Security, Liability Management, Data Management, etc. before introducing features such as payments initiation and account switching.

## Technology and Cyber Security

> *This consultation paper seeks input on how risks related to consumer protection, privacy, cyber security and financial stability should be managed for open banking going forward. Given that the digital transformation presents similar risks across sectors, views are welcome on whether cross-sector or sectoral responses are most appropriate.*

Credit unions are generally supportive of Canada's National Cyber Security Strategy as well as the goals of the National Digital and Data consultations. Financial transactions and payments involve more than just financial institutions and financial service providers such as fintechs, which means in Open Banking system, non-financial actors have a responsibility to protect their customer's data. The introduction of a Digital ID system, whether federated and decentralized, federal, or provincially controlled, should be implemented in lockstep with the implementation of Open Banking in Canada. Just as PIPEDA and provincial privacy legislation may require amendments, a Canada-wide Digital ID infrastructure will allow for the faster socialization and acceptance of Open Banking, as well as easier data portability and an understanding of data rights.

As it is being developed, the CCUA so far agrees with the Pan Canadian Trust Framework (PCTF) document being developed by the DIACC in partnership with government and private organizations. A Digital ID system in Canada that meets the eventual PCTF requirements will serve as a solid foundation for verification and authorization needed for Open Banking data sharing to occur.

The government will need to consider other technology and cyber security aspects in the introduction of Open Banking, including:

- Requiring all participants have auditable data governance policies. That these audits happen on a regular basis to ensure confidence in sharing data.
- A policy to allow participants to request copies of these policies from other participants (where a participant reasonably suspects that something is awry).
- Government and industry oversight on the development of the single, open, standard API to ensure that the API complies with the PCTF.
- Initial certification and regular certification renewal.

- Dedicated technical resources from the regulator reviewing and monitoring Open Banking technical standards to ensure they are continuously secure, and that participants are notified immediately of any vulnerabilities.

- Mandatory immediate breach notification from the affected party.

- The ability for participants to halt or shutdown transactions in the case of a discovered security exploit or hack.

We look forward to discussing these and other technical issues with the government as the regulatory technical standards are being developed.

## Conclusion

- Consumer protection and citizen privacy are paramount in the creation of the Open Banking framework. The socialization and education of Canadians as to their rights and responsibilities when participating in Open Banking interactions will need to be extensive if this innovative concept is to succeed.

- Open Banking should be developed after, or in lock-step, with a modernization of PIPEDA, and provincial consumer privacy legislation. A cross-sectoral Digital ID system should be in place before Open Banking is implemented. The current payments modernization initiative should further develop and mature before payments initiation is within scope of the Open Banking framework.

- The government should define the scope of Open Banking early in the implementation process.

- Open Banking participants must be required to go through a strong certification process that ensures continuous compliance in cyber security and consumer protection. There should be a regular re-certification process.

- Jurisdictional issues between the federal government and provincial governments as they relate to how provincial financial institutions need to be addressed. Provincially regulated credit unions should be allowed to participate in an Open Banking ecosystem because of their market penetration.

- The government should mandate that a single, standard, open API be used for the Open Banking ecosystem. This would help ensure a level playing field and fair competition amongst financial services providers of all sizes.

- The government needs to lay out explicit rules around liability of financial services providers in order to encourage participation in the Open Banking ecosystem, as well as protect consumers and financial institutions.

We thank the government for the opportunity to participate in this process, and look forward to engaging with the government further on Open Banking.