THE ROAD TO CANADA'S OPEN BANKING FRAMEWORK: UPDATES FROM THE WORKING GROUP MEETINGS

Posted on November 2, 2022

Categories: Insights, Publications

Canada's open banking framework is beginning to take form.

Over the past three months, the four working groups assembled earlier this year have been working to develop common rules, accreditation criteria, and technical standards for Canada's open banking system. These working groups are made up of representatives from consumer groups, banks and other prospective open banking participants.[1] Each group focuses on one of four essential elements of Canada's open banking framework: **accreditation**, **liability**, **privacy** and **security**.

Each working group has now had the opportunity to meet five times, and summaries of the first three meetings for each group have been published. This bulletin provides a high-level overview of the outcomes from these first twelve meetings.

Hang on, what is open banking exactly?

Open banking is a system that empowers consumers to direct their financial institutions to share their data with third parties of their choosing. The expected implications of open banking include increased competition, data portability, and the wide proliferation of accredited options for financial tools and services for both consumers and businesses. For financial technology companies, increased access to data from open banking brings the potential for more growth and scalability. Small and medium sized enterprises could also reap many benefits from open banking, including improved technological platforms and greater access to small business financings.

We have been following the development of open banking in Canada closely since the concept first gained traction in 2019. We summarized the Open Banking Advisory Committee's final report ("**Final Report**") in August 2021 and conducted a deep dive on the privacy implications of an open banking framework in October 2021. More recently, we have written about the results of an Open Banking Expo survey, and the appointment of Abraham Tachjian as Canada's open banking lead.

Working Group #1 – Accreditation

What does it take to get in?

The accreditation working group is tasked with developing a framework for accrediting open banking participants, which includes the criteria for accreditation, the process for obtaining accreditation, and insurance or comparable financial guarantee requirements. The goal is to develop a sound, robust, and transparent accreditation process that will mitigate operational, reputational, and concentration (i.e. oligopoly) risks.

The group reached a consensus that the accreditation criteria should focus on four elements: (1) background information and internal governance, (2) financial capacity, (3) certification, and (4) privacy and security. Additional accreditation categories of environmental and social governance (ESG) and anti-money laundering (AML) were also considered, but no agreement was reached on whether these should be included. Of note, the working group took interest in the potential for a framework with different tiers of accreditation, based on factors such as size or role of the prospective participant.[2]

In order to promote an accountable system, participants must have the financial capacity to meet their liabilities. The group came to a general consensus that an adequate insurance policy or comparable financial guarantee would be required in order to obtain accreditation. The group came to a general consensus in favour of Australia's flexible approach in this regard, which evaluates the adequacy of an insurance policy based in part on (i) the nature of the products or services to be offered, (ii) the nature of data to be managed, and (iii) the volume of data to be handled.[3]

Working Group #2 – Liability

What happens when something goes wrong?

The liability working group is developing rules to allocate responsibility when something goes wrong. This includes establishing (i) the process for consumer complaints, (ii) rules to apportion liability, and (iii) traceability frameworks.

The working group agreed that when a consumer suffers a loss in the course of exercising any function of open banking, the consumer should not be liable for more than a nominal fee of $50, unless it can be proven that the consumer committed gross negligence, gross fault or fraud.[4] A majority of group members agreed that the data recipient should be required to automatically compensate consumers who suffer financial harm, though a pooled fund between all open banking participants was also considered.

One objective of the group was creating a standard approach to protecting consumers following a sensitive data breach. Group members discussed the importance of active and ongoing measures such as credit monitoring services, shutting down compromised accounts, changing account numbers, and transparency of

root cause investigations.[5]

The working group also considered approaches to a traceability framework for the open banking system to facilitate monitoring and create audit trails for data-in-transit. The group agreed upon a decentralized approach (i.e. one without a government data intermediary). The group also agreed that all data recipients should have obligations for data traceability when facilitating consumer data requests and that data recipients should be responsible for open banking data even if they outsource their business operations. The group proposed that data recorded for traceability purposes should include user consent, flows of data, as well as the dates of each data-sharing request.[6]

Working Group #3 – Privacy

How will consent be managed?

The privacy working group is developing rules for how consumers provide and revoke consent to share their data, and how consumer data can be used pursuant to the consent provided.

The working group agreed that an approach to consent should align with privacy standards already established for the financial services industry, including federal and provincial privacy laws.[7] The working group also agreed that the process for giving or withdrawing consent should be clear, simple and transparent, to promote a positive consumer experience. The consumer should be able to quickly withdraw consent with either the data recipient or the data provider (which would need to communicate among themselves to enact the withdrawal). The group also discussed making revocation of consent automatic under certain circumstances, such as when a consumer closes their account, or when the purpose for which the consumer's data was collected changes.

The working group also discussed requirements for public disclosure of useful information for consumers (e.g., terms and conditions, service agreements, complaint procedures, etc.) and agreed that the principles of the Financial Consumer Protection Framework, which already apply to banks and other financial institutions, would serve as a good baseline for these requirements.[8]

Working Group #4 – Security:

How will data be protected?

The security working group is developing rules to establish baseline security requirements for open banking participants, particularly in light of the data security, cyber security and operational risks of open banking. Of note, the working group is not tasked with evaluating the technical standards of the application programming interface (API) which will facilitate data exchange between open banking participants. Instead, the open

banking lead will conduct separate due diligence on this element, with support from the Department of Finance Canada.

After assessing various existing frameworks and certification regimes (including ISO27001 and SOC 2), a majority of the working group agreed that the National Institute of Standards and Technology ("**NIST**") framework was the best option. In particular, the NIST framework allows for various compliance tiers, and addresses both information security and cyber risk.[9]

The group identified some drawbacks with the NIST framework however, including the fact that (a) compliance may be challenging for smaller participants, (b) significant time and resources may be required for implementation, framework modifications, and additional controls, and (c) NIST framework expertise in the market is relatively low. The group considered that most of these concerns could be mitigated with early and clear communication to allow the market to adjust.[10]

Key Takeaways

- The working groups have demonstrated a strong priority for consumer education, consumer protection, and a positive user experience. These elements are essential for strong uptake in the open banking system.
- There is a clear push for flexible, self-determined requirements, in order to accommodate a variety of open banking participants. In particular, there was a general consensus in favour of establishing different tiers of accreditation requirements.
- The working groups are not trying to reinvent the wheel. Where possible, they are drawing from existing legislation and frameworks, including the *Competition Act*, existing regulatory guidance, the Financial Consumer Protection Framework, and the NIST framework.

Timing and Next Steps

Each working group is planning to meet several more times to further develop the open banking framework, and according to the Department of Finance, the term of each working group is expected to end by September 29, 2023.[11] It therefore seems likely that open banking will not be available until the end of 2023 or early 2024, rather than the federal government's stated goal of early 2023.[12]

We will provide further updates when more information is available.

[1] The working groups have been criticized recently for lack of consumer perspective: see Vass Bednar and Robert Fay, *If open banking is for consumers, why are they missing from the discussion?* *(October 3, 2022)*, Financial Post. The accreditation and security working groups lack any consumer representatives among their membership. Consumer representatives make up only 14% of the liability working group's composition and

only 15% of the privacy working group's composition. A government consumer advocacy agency (The Financial Consumer Agency of Canada) also participated in each working group meeting, but in each case as an external guest.

[2] Department of Finance Canada, "Accreditation working group meeting 2 – July 27, 2022" (August 18, 2022).

[3] Department of Finance Canada, "Accreditation working group meeting 3 – August 23, 2022" (August 23, 2022).

[4] Department of Finance Canada, "Liability working group meeting 1 – July 7, 2022" (July 7, 2022).

[5] Department of Finance Canada, "Liability working group meeting 2 – July 26, 2022" (July 26, 2022).

[6] Department of Finance Canada, "Liability working group meeting 3 – August 18, 2022" (September 26, 2022).

[7] Department of Finance Canada, "Privacy working group meeting 2 - July 25, 2022" (August 16, 2022).

[8] Department of Finance Canada, "Privacy working group meeting 3 – August 16, 2022" (September 26, 2022).

[9] SOC 2 certification was viewed as too elementary whereas ISO27001 was considered too stringent.

[10] Department of Finance Canada, "Security working group meeting 2 – July 28, 2022" (August 18, 2022).

[11] Department of Finance Canada, "Terms of reference for the open banking working groups and steering committee" (July 7, 2022).

[12] Federal Liberal Government 2021 platform *Forward. For Everyone*. s.v. "A Fairer Financial System".

by Darcy Ammerman, Robbie Grant, Mitch Koczerginski, Robert Piasentin, Pat Forgione, Isabelle Guevara, and Kendra Wilson (Articling Student)

A Cautionary Note

The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned against making any decisions based on this material alone. Rather, specific legal advice should be obtained.