http://www.fdata.global/north-america

June 29, 2022

Mr. Peter Routledge
Superintendent
Office of the Superintendent of Financial Institutions
255 Albert Street
12th Floor
Ottawa, Ontario KIA OH2

Sent via electronic mail to b10@osfi-bsif.gc.ca

Re: Office of the Superintendent of Financial Institutions Public Consultation on Draft Guideline B-10: Third Party Risk Management Guideline

Dear Superintendent Routledge:

The Financial Data and Technology Association of North America ("FDATA North America") appreciates the opportunity to submit comments in response to the Office of the Superintendent of Financial Institutions' ("OSFI") public consultation on Draft Guideline B-10: Third Party Risk Management.

FDATA North America was founded in early 2018 by several financial firms whose technology-based products and services allow consumers and small and medium enterprises ("SME") to improve their financial wellbeing. As the leading trade association advocating for customer-permissioned access to financial data, FDATA North America's members include firms with a variety of different business models. Collectively, our members provide millions of Canadian consumers and SMEs access to vital financial services and products, either on their own or through partnerships with supervised financial institutions. Regardless of their business model, each FDATA North America member's product or service shares one fundamental and foundational requisite: the ability of a customer to actively permission access to some component of their own financial data that is held by financial services providers.

FDATA North America's members include both service providers to banks and technology platforms that are not bank service providers. As a result, we limit our feedback to the B-10 draft to the interplay between OSFI's draft guidelines and the development and implementation of an open banking framework in Canada, which the Department of Finance intends to launch in the next 18 months, led by the newly-appointed Open Banking Lead.

Importance of Distinguishing Third-Party Providers from Open Banking Providers

Digitalization and financial technology have brought increasing complexity to the financial system, particularly regarding the nature of entities' relationships to FRFIs. Among those

changes has been the rise of Open Banking, which refers to consumers' ability to access and share their financial information with companies who provide them with financial products and services, which has introduced new entrants who provide ancillary services like lending, budgeting, automatic savings, and investing.

As it is OSFI's mandate to keep FRFIs and, by extension, Canada's financial system, safe, sound, and secure, it is critical to distinguish third-party providers who directly work with FRFIs from providers serving consumers and/or SMEs whose only relationship with a FRFI is accessing data about that consumer and/or SME, with their permission, to provide the customer with the benefit of their product or service (what we call here "customer-selected providers").

Historically, third-party providers to FRFIs included either vendors for internal processes, or formal partners delivering services directly to customers. Under an open banking model, however, customers initiate financial relationships with entities who do not have formal relationships with their financial institutions. These relationships tend to mirror those customers may have with mortgage, insurance, or credit card providers, who obtain customer financial information in order to offer services but are not themselves third parties to FRFIs. The only distinction is that while historically those third parties may have obtained consumer information via a consumer printing out their account information, under open banking that activity is carried out programmatically - data aggregation is essentially the digital version of carrying a shoebox of receipts to your tax preparer.

Critically, for the purposes of risk management, FRFIs lack any direct relationship with the customer-selected providers with whom their customers interact - and in some instances may have none at all. For example, a customer might leverage a data aggregation service to provide their account information to a budgeting application so that they can better track their finances. While a FRFI may have a relationship with the data aggregator who is performing the function of data portability on behalf of that customer, it most likely does not have a relationship with that budgeting application, and therefore could not reasonably oversee or be responsible for its operations. Moreover, in many instances, FRFIs are themselves consumers of customer-permissioned data.

OSFI cannot reasonably expect one FRFI, acting as a data provider in an open banking environment, to exert third-party risk management over a competing FRFI, who may be acting as a data recipient in an open banking environment. The only appropriate method for ensuring safety and security for the open banking regime is to provide for robust open banking accreditation standards that any data recipient must meet in order to gain access to the system, and to require that no data provider may restrict access to customer-permissioned data from an accredited open banking provider.

Interplay Between B.10 and Development of Open Banking in Canada

OSFI proposes in its draft guidelines to define a "third-party arrangement" as "any business of strategic arrangement between a federally regulated financial institution ("FRFI") and an entity(ies) or individual(s), by contract or otherwise." The broad scope of this definition could capture virtually any third party that has any interaction with a FRFI, other than FRFI customers, which are explicitly excluded. Moreover, because third-party risk management guidelines are left to FRFIs to interpret and apply, this proposed definition would unquestionably lead to disparate outcomes, with some FRFIs classifying certain third-party activities as covered under the definition while others may not.

We appreciate the clarification provided by a footnote at the end of the consultation, which recognizes that this draft guideline is not intended to impede the establishment of an open banking framework for Canada. Unfortunately, the footnote alone does not satisfactorily address the need to ensure coordination of accreditation for open banking providers. Beyond the draft definition itself, the inclusion of "loss of data by a third party" as a specific third-party risk proposed to be covered under the guidelines would seem to require FRFIs to extend third-party oversight to providers in an open banking ecosystem, despite what we believe to be the intention of the footnote at the end of the document.

Without amendment, this construct has the very real potential to, at best, undermine the standardization of open banking accreditation, and, at worst, to completely undercut an open banking accreditation regime in favor of FRFIs' interpretations of OSFI's third-party risk management requirements. Any overlap between these two regimes – B-10 and open banking accreditation – will cause tremendous and unnecessary confusion amongst both FRFIs and open banking providers, and will significantly hinder the development of open banking across Canada. We therefore suggest that the most appropriate amendment to address this critically important issue would be to make unambiguously clear that accredited open banking providers under Canada's open banking system are exempt from OSFI's third-party risk management framework.

In countries that have deployed open banking regimes more quickly than Canada, including the United Kingdom, Australia, New Zealand, and Singapore, we have witnessed regulators achieve safety and soundness, customer protection, and the innovation brought to bear by a customer-centric model in which end users may seamlessly share their data with third parties. For example: in the United Kingdom, where open banking just celebrated its fourth birthday, five million individual users interact with open banking use cases each month[1] in a safe and secure ecosystem in which no third-party breaches have occurred. In the UK, any open banking provider must first be approved under the Financial Conduct Authority's accreditation standards before offering its product or service to consumers or SMEs. In Australia, only providers accredited by the Australian Competition and Consumer Commission ("ACCC") can offer services using its open banking platform, and all accredited providers are listed on a central directory, along with their accreditation number, status as a data holder or recipient, and contact information. The ACCC

[1] Open Banking UK News: "Five Million Users-Open Banking Growth Unpacked." Published Feb. 24, 2022

has developed clear and detailed guidelines[2] for providers on how to gain accreditation, lists the step-by-step process, and provides sample application forms. The rigorous work completed by these countries, along with the recommendations in the Advisory Committee Report, provide Canada's policymakers with both guidance and confidence that a fully secure and functional open banking system that includes an accreditation process can be delivered in relatively short order.

The framework articulated in the Minister of Finance's Advisory Committee on Open Banking's recommendations, which the government and the Open Banking have endorsed, proposes minimum accreditation requirements for open banking providers to gain access to the system. Accreditation of financial services providers is an important element of the Advisory Committee's suggested framework that can bring fintech providers into a well-structured open banking system, and one to which FDATA North America and its members are steadfastly committed for Canada.

As OSFI develops its guidelines for third-party technology partners to banks, we respectfully offer that significant consideration has already been undertaken on this issue by the Department of Finance and all involved in development of the open banking framework. At this time, all stakeholders in the open banking ecosystem would benefit from more detailed public documentation that clearly delineates OSFI's authority and responsibilities with regard to third-party financial technology providers to FRFIs from those of the Department of Finance for open banking providers as the work to build and deploy a Canadian open banking regime enters a crucial phase.

OSFI should create a specific carveout from B-10 for all accredited open banking providers under Canada's open banking framework as part of this consultation, and before the new open banking system is implemented. To the extent that OSFI is concerned that Canada's final open banking framework fails to include an accreditation regime, we would respectfully offer that adding this exemption to B-10 would have no practical impact in such an eventuality, as there would not in that outcome be any accredited open banking providers.

Conclusion

The future of customer-selected financial technology providers is dependent on their ability to work with customers to offer innovative digital products. To facilitate enhanced market competition and customer choice, it is imperative that OSFI collaborate with the Department of Finance and the Open Banking Lead to harmonize regulatory expectations and clarify in the strongest possible terms that open banking providers accredited under Canada's forthcoming open banking regime are exempt from the requirements established by this consultation.

[2] Australian Government. "Consumer Data Right Accreditation Guidelines Version 3." Published Feb. 2022

http://www.fdata.global/north-america

Thank you in advance for your consideration of our perspectives.

Sincerely,

Steven Boms
Executive Director