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

February 7, 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 Tech.Cyber@osfi-bsif.gc.ca.

Re: Office of the Superintendent of Financial Institutions public consultation on Draft Guideline B-13: Technology and Cyber Risk Management.

Dear Superintendent Routledge:

The Financial Data and Technology Association of North America ("FDATA North America") appreciates the opportunity to submit comments to the Office of the Superintendent of Financial Institutions' ("OSFI") public consultation on Draft Guideline B-13: Technology and Cyber Risk Management.

About FDATA North America

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, and because most of our members are not directly supervised by OSFI, we limit our feedback to the B-13 draft to two critical areas for the third-party financial provider community: the interplay between OSFI's draft guidelines and the Department of Finance's work on open banking, and the draft's discussion regarding third-party provider technology and cyber risk.

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

Interplay Between B.13 and Development of Open Banking in Canada

Our members, which include some of the most innovative and widely used financial technology companies across the country, have been encouraged by recent signals from the federal government, namely the Department of Finance, that Canada will soon implement an open banking regime. Following the release of a report from the Advisory Committee to the Minister of Finance on Open Banking last August, the federal election saw commitments pledged from across the political spectrum for the delivery of open banking in Canada next year.

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 balance 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, four million individual users interact with open banking use cases each month in a safe and secure ecosystem in which no third-party breaches have occurred. FDATA expects Canada to strike this balance through the framework articulated in the Advisory Committee Report, which proposes minimum accreditation requirements for third-party 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.

Open banking accreditation standards in Canada will almost certainly include cybersecurity requirements for third-party providers. Harmonization of efforts between the Department of Finance's open banking work and OSFI's approach to third-party cybersecurity risk will therefore be essential. As OSFI develops its technology 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 stakeholders would benefit from some form of public documentation that clearly distinguishes OSFI's authority and responsibilities with regard to third-party financial technology providers from those of the Department of Finance as it works to implement a Canadian open banking system. Publicly clarifying how these two projects will interact will provide clear direction to the marketplace about how third-party providers can continue to offer their valuable financial services and products in an innovative, competitive marketplace.

Distinguishing Third-Party Providers from Customer-Selected Providers

Digitalization and financial technology have brought increasing complexity to the financial system, particularly regarding the nature of entities' relationships to federally regulated financial institutions ("FRFIs"). As it is OSFI's mandate to keep FRFIs safe, sound, and secure, it is critical to distinguish third-party providers who directly engage with FRFIs from providers

serving consumers and/or SMEs without a formal relationship to their customers' primary financial institution (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.

Critically, for the purposes of risk management, FRFIs lack insight into the customer-selected providers with whom their customers interact. 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 that 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 its cybersecurity practices. FRFIs in an open banking regime most often interact with data aggregators performing data portability functions via customer authorization, and therefore it is those data aggregators, and not the customer-selected fintech applications who may serve, playing the role of a third-party to an FRFI. In some instances, FRFIs are themselves consumers of customer-permissioned data via data aggregators. In these instances, it is clear that data aggregators are third parties to FRFIs and would fall under the B-13 framework.

OSFI should clarify that providers with whom customers engage directly, without any intervention from their FRFI, do not fall under the B-13 framework. In an increasingly digital and data-driven ecosystem, in which technologies like data aggregation allow consumers and SMEs to easily transmit their financial information across providers, bringing all providers with whom consumers interact under the third-party risk management umbrella would overburden FRFIs with risk management requirements over firms with whom they do not hold any formal relationship.

Tailored Approach to Third-Party Cyber Risk Management

As OSFI works to foster development of partnerships between FRFIs and third parties, we offer that the primary goal of this consultation should be to ensure that FRFIs third-party risk management requirements mirror their ability to oversee entities with whom they have direct relationships, and not to overburden FRFIs with system-wide oversight that instead should fall to a collaborative regulatory effort including Finance Canada's open banking accreditation regime. A properly devised policy must also guard against the risk of becoming a gatekeeping device that would serve to stifle competition, particularly when many customer-selected providers offer products and services that a customer's bank may not offer, or to customers that a bank may not service. To right-size oversight requirements for FRFIs, it is critically important that OSFI

develop clear and objective standards regarding the cyber risk management requirements, particularly those associated with financial data sharing. These efforts should be conducted in the most transparent means possible, and we would be happy to provide guidance and assistance to ensure the outcome of this consultation strikes the appropriate balance.

Our members are increasingly concerned that as we await the impending launch of an open banking regime, FRFIs may leverage B-13 to override customer direction to share their financial data. A third-party provider technology and cyber risk framework that allows the FRFI to define, implement, and police its own standards, as section 4.1.2 of the proposed guidance suggests, has the potential to significantly alter the shape of today's financial services marketplace.

Even before OSFI's proposed guidance has been finalized, customer-selected providers in Canada are experiencing a range of restrictions to customer-permissioned data that includes selective blocking of specific use cases, degradation of data, and targeted blocking of sharing specific data fields. In each of these cases, the ability of the third-party provider to offer its services to the consumer or SME is significantly curtailed or completely restricted. Accordingly, competition in data-driven financial services is already being substantially inhibited to the severe detriment of consumers and SMEs. This undesirable balance of power derives from the existing approach to third party risk responsibility, which allows FRFIs to unilaterally create security standards which can be deployed toward anticompetitive ends.

We are deeply concerned that section 4.1.2 of the proposed guideline underscores existing policies that have led to the market distortions described above. If FRFIs are further shouldered with responsibility for customer-selected providers' cybersecurity compliance as proposed in this section, we would expect further restrictions on customer-selected providers' access to customer-permissioned financial data, which would directly conflict with the established policy goals of Canada's open banking journey. To be clear: we are not suggesting that customer-selected financial providers should escape appropriate oversight; in fact, FDATA North America has always held the position that customer-selected providers should be responsible for the security of the customer data that they access, must accept any liability responsibility arising from cybersecurity breaches, and be able to fulfill any required customer redress. On multiple occasions in fact, we have led efforts urging government agencies to proactively develop uniform standards, which the market on its own has not been able to establish.

Front-running an open banking regime by force-fitting customer-selected oversight into third-party oversight will unduly burden FRFIs with risk management responsibilities they may not in fact be able to carry out, and for which their only recourse may be to shut down their customers' access to data portability, which are grounded in Canada's Digital Charter.

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

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 work with the Department of Finance to harmonize regulatory expectations of customer-selected financial providers as open banking takes hold in Canada. As part of this effort, we strongly request that OSFI consider the impact to market structure and the ability of FRFIs to manage risk in a system in which they do not hold direct third-party relationships with all entities offering consumers and SMEs financial products and services.

Thank you in advance for your consideration of our perspectives.

Sincerely,

Steven Boms
Executive Director