www.fdata.global/north-america

FDATA North America Response to Retail Payments Supervision Consultation

Comments to be submitted via RPSconsultationsSPD@bank-banque-canada.ca

The Financial Data and Technology Association of North America ("FDATA North America") is broadly supportive of the objectives of the regulations to implement the Retail Payment Activities Act ("the Act"). Our member companies, which include financial technology firms, customer-permissioned data aggregation platforms, and providers of financial services and tools to Canadian consumers and small and medium enterprises, have since our inception been united behind the notion that a well-regulated financial services marketplace must balance customer protection on the one hand and innovation on the other. Adoption of these proposed regulations would see as many as 2,500 payment service providers ("PSPs") overseen under a strong regulatory framework and would, once finalized and implemented, meaningfully advance the modernization of Canada's financial services marketplace. As both the Department of Finance and the Bank of Canada are well aware, a significant majority of G7 nations have both already adopted regulatory regimes for non-bank PSPs and implemented open finance frameworks.

FDATA North America would respectfully suggest that the implementation of these regulations should facilitate an expedited inclusion into the scope of Canada's consumer-driven banking framework of payment use cases. As you know, Deputy Prime Minister and Minister of Finance Chrystia Freeland last month introduced the government's 2024 budget, which included the framework that will deliver consumer-driven banking in Canada.[1] The vision for the design of consumer-driven banking outlined the scope of data that will be covered, to include chequing and savings accounts, investment products, and lending products. Minister Freeland emphasized that the government may consider an expansion of the scope in future iterations to include additional data, entities, entry processes, and functionalities, such as the ability to initiate payments. This aligns with the final report, released in 2021 by the Minister of Finance's Open Banking Advisory Committee, which recommended that "future expansion of the open banking system to include payments should be considered in the context of payment modernization to ensure alignment with that framework."[2] With a supervisory regime for PSPs in place once these regulations have been finalized, a key component of payment modernization will have been delivered. Moreover, as a result of the delivery of the first phases of Canada's open finance framework in the Budget Implementation Act, incorporation of payment initiation use cases into Canada's open banking framework will be implemented at the beginning of Canada's open finance journey.[3] FDATA North America therefore encourages the Bank of Canada to consider regulated PSPs in the implementation of Canada's open banking framework, particularly as it pertains to payment initiation use cases. By leveraging the finalized regulatory framework for PSPs, Canada can expedite the integration of these entities into its consumer-driven banking system, ensuring alignment with the broader objectives of payment modernization and the principles outlined in the Open Banking Advisory Committee's final report.

[1] Budget 2024: Canada's Consumer-Driven Banking Framework - Canada.ca
[2] Final Report - Advisory Committee on Open Banking - Canada.ca
[3] nwmm-amvm-0424-bil.pdf (canada.ca)

FDATA North America values the opportunity to provide input on the updated supervisory guidelines under the Act. As we analyze the guidelines, it becomes evident that certain clarifications are necessary to ensure they accommodate the varied operational models within our membership.

Response to Operational Risk and Incident Response

The Act's Operational Risk and Incident Response guidelines warrant a nuanced approach, particularly regarding the standard of due diligence expected of outsourced service providers within the PSP network. A comprehensive checklist or ongoing audit attestation process would aid PSPs in assessing and maintaining compliance. Due to varying operational models and unique exposure levels to risks such as security breaches, regulatory non-compliance, financial fraud, system outages, and supply chain vulnerabilities, a universal threshold for allowable operational risk may not be feasible. Clear thresholds in Appendix A would help distinguish between "ubiquitous" and "more interconnected" PSPs, with a defined test for these categories guiding the adoption of the three lines of defense risk management approach.

Regarding the requirement for PSPs to report material breaches to all relevant parties within 24 hours, we identify significant operational challenges. This timeframe can be particularly constraining when engaging in necessary communications with end-users and conducting essential fact-finding activities. We suggest that the guidelines allow for a longer reporting period, giving PSPs sufficient time to gather accurate information and communicate effectively with all affected parties. Extending the reporting timeframe would help PSPs maintain transparency and accountability, acknowledging the complexities of comprehensive incident response without compromising the quality and integrity of the communication.

For reliability targets, such as availability, recovery time objective, recovery point objective, and maximum tolerable downtime, a baseline standard is essential to ensure consistency across PSPs. Furthermore, guidelines should define a baseline minimum for prompt detection, offering criteria to determine what constitutes timely detection. Additionally, the testing of controls should include flexibility, allowing for SOC II Type 2 audits or similar standards, while also ensuring that specific PSP control procedures are covered. In terms of compensating controls, additional guidance is needed to support smaller PSPs facing larger outsourced service providers, particularly in monitoring and termination plan execution.

Lastly, further clarity is crucial regarding expectations for monitoring affiliate entities of outsourced service providers. This requirement could be overly cumbersome, given that many affiliates may not be directly involved in service provision, potentially making compliance challenging with little or no corresponding risk management benefit.

Response to Incident Response

FDATA North America proposes a streamlined approach to incident reporting involving personal information. Currently, PSPs are required to report such incidents both to the Bank of Canada and the Office of the Privacy Commissioner (OPC). To reduce duplicative reporting and administrative burdens, we recommend that PSPs be required to report these incidents solely to the OPC. In turn, the Bank of Canada should receive updates through an information-sharing Memorandum of

Understanding (MOU) with the OPC. This modification would allow PSPs to focus their resources more effectively on incident management, ensuring compliance while enhancing operational efficiency and data protection.

Response to Safeguarding End-User Funds

FDATA North America's member companies that facilitate transactions without directly managing end-user funds believe clarity is necessary on the definition of "holding funds" within the guidelines. We recommend that the guidelines clearly exclude firms involved only in transmitting data or facilitating transactions but that do not actually hold end-user funds. Such clarification would help these firms precisely understand their specific obligations and exemptions under the new regulatory framework.

Moreover, it is important to delineate the scope of responsibility for firms that do not hold funds. Detailed guidance on how the guidelines apply to these firms in terms of compliance, risk assessment, and reporting requirements are necessary. Without these clarifications, non-holding entities might face significant challenges in implementation. Specifically, aligning with safeguarding requirements designed primarily for entities that hold funds could be both operationally and financially burdensome. Additionally, the expectation for maintaining detailed records, conducting periodic reviews, and managing comprehensive compliance frameworks could impose considerable administrative overhead.

Response to Notice of Significant Change or New Activity

On this score, clarity is needed on whether changing from one cloud provider to another qualifies as a "change in technology" necessitating notification to the Bank of Canada. This process can vary significantly based on the extent of the transition, the impact on operational risk, and the sensitivity of data involved. The guidelines should explicitly define the criteria under which cloud migration warrants notification, considering factors like changes in security protocols, data handling practices, or integration frameworks. Clear guidance will help PSPs better understand when such a change is deemed significant enough to inform the Bank of Canada, ensuring compliance while managing operational risks efficiently.