



www.fdata.global/north-america

DRAFT

June 14, 2023

FDATA North America Responses to PSP Association Outreach and Roundtable: Key Retail Payment Supervision Registration (“RPS”) Concepts

Introduction

The Financial Data and Technology Association of North America (“FDATA North America”) appreciates the opportunity to provide its perspectives in response to the Bank of Canada’s (“the Bank”) request for further input regarding key registration concepts associated with implementation of the Retail Payments Activities Regulations (“the Regulations”). As we shared in our formal submission in response to the proposed Regulations earlier this year, 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 (“SMEs”), are broadly supportive of the objectives of the Regulations, and several FDATA North America member companies will ultimately count themselves among the 2,500 payment service providers (“PSPs”) subject to the registration regime imagined under the proposed Regulations.

At the Bank’s request, FDATA North America has consolidated the feedback we received from our members to paper discussing considerations for key RPS registration concepts. Our members’ feedback principally focused on three areas of the paper: the Bank’s interpretation of the of the term “end user” under the Retail Payments Activities Act (“RPAA”); concerns regarding the impacts of tokenization; and, a desire for clarification that data intermediaries meet the Bank’s interpretation of “incidental” under the Regulations.

Definition of “End User”

The Bank notes in its paper that the RPAA defines “end user” as an individual or entity that uses a payment service as a payor or payee. As described in the paper, the Bank is proposing definitions of “payee” and “payor” such that “payee” means a natural or legal person who is the intended ultimate recipient of funds which have been the subject of an electronic funds transfer and “payor” means a natural or legal person who orders an electronic fund transfer (“EFT”) to take place and who is the initial source of the funds for that EFT. FDATA North America’s members provided two recommendations to the Bank in response to these proposed interpretations.

First, FDATA North America’s members suggest that the Bank amend its proposed definitions of “payee” and “payor” to clearly include entities in addition to natural or legal persons, or that the Bank reference a statutory definition of legal persons that makes unambiguously clear that small and medium-sized enterprises (“SMEs”) will be covered within the scope of the proposed



www.fdata.global/north-america

DRAFT

definitions. This recommendation would make clear that SMEs would derive the same benefits and protections from the implementation of the Regulations as would individuals, which FDATA North America believes aligns with both Parliamentary and the Bank’s intent.

Second, FDATA North America’s members encourage the Bank to add “or an individual or entity acting on behalf of a natural, legal person, or entity” to its proposed interpretations of the definition of “payee” and “payor” within the Regulations. Inclusion of this language will ensure that individual consumers and SMEs derive the same rights and protections whether they themselves are engaging with a PSP or whether an individual or entity is doing so at their direction, including, for example, an accountant, a family member, or a financial professional. Moreover, clarity that individuals or entities acting on behalf of end users meet the definition of a “payee” and a “payor” under the Regulations will proactively address potential regulatory uncertainty for PSPs and data intermediaries once the Regulations have been fully implemented.

Tokenization May Impair End User Authentication and Thwart Use Case Access

In its paper, the Bank asks whether tokenization may affect a PSP’s or data intermediary’s ability to identify an end user. While implementation of more secure account access technologies is unquestionably in the best interests of Canadian consumers and SMEs, based on FDATA North America’s members’ experiences in other jurisdictions in which tokenization has been deployed, our members would respectfully offer that a transition to tokenized account access should be undertaken thoughtfully and in a manner that ensures that the end user is always in full control of their financial data.

Token-based authentication regimes have become increasingly more commonplace in jurisdictions in which open banking has advanced more quickly than it has in Canada. In the United States, for example, several of the largest financial institutions have deployed OAuth-enabled tokenization authentication protocols to facilitate access to application programming interface gateways for the purpose of enabling more secure customer-permissioned data sharing. By definition, token-enabled authentication flows allow the financial institution with which an end user has a primary banking relationship to determine whether or not to authenticate the end user and thus to allow them to connect to a third-party provider. It is therefore essential that the Regulations mirror the authentication requirements FDATA North America’s member companies operate under in other jurisdictions, including the United States, which make clear that authentication may not be used as a means to stifle competition or to prevent end users from choosing to engage with registered PSPs.

While perhaps not the direct focus on the Bank’s question on this score, FDATA North America would also volunteer that some financial institutions have in other markets sought to tokenize specific data fields, including account and routing numbers. While these efforts have been rationalized by the financial institutions as a means of further securing sensitive customer data,



www.fdata.global/north-america

DRAFT

they have, in practice, served only to restrict those financial institutions' customers from accessing a more competitive PSP marketplace. Such an outcome in Canada would be directly contrary to the goals of both the RPAA and the Department of Finance's forthcoming open banking framework, which both aim to put the end user in control of choosing the service provider best suited to their unique financial situation in a safe and secure ecosystem.

The Bank Should Clearly Assert that Data Intermediaries Are Not PSPs

The RPAA defines "payment services provider" as an individual or entity that performs payment functions that are not "incidental" to another service or business activity. In its paper, the Bank proposes a framework to guide its analysis of whether a payment function is being performed in a manner that is "incidental" to other services or business activities, however the Bank's proposed analytical framework does not make clear whether customer-permissioned data intermediaries, which sit between financial institutions and PSPs to provide data connectivity between the two entities, will be required to register under the Regulations.

Customer-permissioned data intermediaries may in some cases facilitate one or more of the five payment functions as described by the Bank, namely transmitting authorization of an instruction in relation to an EFT when requested to do so by a PSP that has received such authorization from an end user. Data intermediaries, however, provide materially similar customer-permissioned data connectivity for non-payment use cases in both Canada and globally and, in instances in which they are providing end user-permissioned data connectivity on behalf of a PSP, have no direct relationship with the end user for the purpose of provisioning payment-related services. FDATA North America's members therefore request that the Bank specifically assert that data intermediaries meet the "incidental" criteria under the proposed Regulations when merely providing user-permissioned data access.