

JUNE 1, 2021

## Modernizing Canada's Retail Payments Ecosystem: Draft *Retail Payments Activities Act* Introduced

Authors: [Zain Rizvi](#) and Gillian R. Stacey

The year 2020 will be remembered as a watershed for many reasons, including being the year that the world was forced to move online to an extent never seen before. Online commerce rose to stratospheric levels in 2020 – Amazon's earnings report for the fourth quarter of 2020 showed that it was the highest quarter ever by revenue, generating US\$125.56 billion in sales. All forms of contactless payment became not just convenient but necessary, and while overall spending by consumers decreased, online spending with its corollary of electronic payments increased. Payments Canada reported that in 2020 electronic payments accounted for 77% of all transactions and that on the retail side, consumer behaviour showed what may be a permanent increase in electronic forms of payment.

To date, financial technology (fintech) companies operating in the retail payments space in Canada (other than regulated financial institutions such as banks) have enjoyed only light oversight from financial services regulators, with many payment providers falling outside the reach of both the federal *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (Proceeds of Crime Act) and *Québec's Money-Services Businesses Act*. The federal government had been monitoring the changes in technology and the lack of regulation in the payments space even before the explosive e-commerce growth of 2020. On April 30, 2021, as part of budget Bill C-30, the government released a draft *Retail Payments Activities Act* (RPAA). The RPAA follows the recommendations made by the Department of Finance in its 2017 consultation paper calling for a new retail payments oversight framework to ensure the protection of end users and to build confidence in the retail payments ecosystem in Canada.

Although not yet finalized, the RPAA may subject most fintech companies operating in the retail payments space to a new regulatory regime under the supervision of the Bank of Canada (BoC), including a registration process that may be subject to national security review and ongoing operating requirements.

### Application of the RPAA

The RPAA will apply to any retail payment activity that is

- i. performed by a payment service provider that has a place of business in Canada; or
- ii. performed for an end user in Canada by a payment service provider that does not have a place of business in Canada but directs retail payment activities at individuals or entities in Canada.

A "payment service provider" (PSP) is an individual or entity that performs payment functions as a service or business activity that is not incidental to another service or business activity. This broadly drafted definition may necessitate some regulatory guidance on whether a particular activity is considered incidental.

Similar to the Proceeds of Crime Act, the RPAA is intended to have extraterritorial effect and will apply not only to PSPs in Canada but also to foreign PSPs that direct retail payment activities at persons located in Canada. Accordingly, foreign PSPs must carefully review their retail payment activities when directed at Canadian customers. Directing services at persons in Canada may include targeted marketing or advertising; using a ".ca" domain name; or being listed in a Canadian business directory.

### What Constitutes Retail Payment Activity?

“Retail payment activity” is defined as a payment function performed in relation to an electronic funds transfer that is in Canadian currency or another country’s currency or using a unit that meets prescribed criteria. While such prescribed criteria will likely be set out in the RPAA’s implementing regulations, the term “unit” may be interpreted broadly to include virtual currencies (such as bitcoin and other cryptocurrencies). Similarly, “payment function” is broadly and generously defined in terms that will require some clarification in the regulations or by the regulator in order to determine which activities are caught by the RPAA and which are not.

### Which Activities Are Excluded?

The RPAA specifically excludes the following retail payment activities from its scope:

- **Banks and other regulated entities:** payment functions performed by a bank; an authorized foreign bank; a credit union; a provincial government or an agent thereof if they accept deposits transferable by order; an insurance company; a trust company; a loan company; the Canadian Payments Association; the BoC; or prescribed individuals or entities;
- **Prepaid payment products:** electronic fund transfers through an instrument issued by a merchant – or a non-PSP that has an agreement with a group of merchants) that allows the holder to purchase goods or services only from the issuing merchant or merchants in such group (e.g., closed loop gift cards);
- **ATM withdrawals:** cash withdrawals at an automatic teller machine;
- **Eligible financial contracts:** a payment function performed to give effect to an “eligible financial contract” as defined under the *Canada Deposit Insurance Corporation Act*;
- **Designated systems:** electronic fund transfers performed by systems designated under the *Payment Clearing and Settlement Act* (this includes the newly designated Interac e-transfer system);
- **Internal transactions:** payment functions performed wholly between a PSP and its affiliated entity; or
- **Agents of PSPs:** agents of registered PSPs performing retail payment activities in the scope of their authority as agents.

Further exemptions from the RPAA may be prescribed in the regulations.

### Registration Under the RPAA

Once the RPAA is in force, a PSP must register with the BoC before it performs any retail payment activities. Applications for registration must contain prescribed information, including details about the services to be provided, a description of the PSP’s operational risk management and incident response framework, the safeguards in place to protect end user funds, and whether the PSP is registered with the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC).

The BoC may refuse or revoke registration for several reasons, including if the applicant provides false or misleading information, is not registered as a money services business (MSB) under the Proceeds of Crime Act where required to do so or has been issued with a notice of violation under the Proceeds of Crime Act in respect of a violation that is classified as “serious” or “very serious.” However, whether an entity is required to register as an MSB can be a matter of debate, turning on whether the provision of money transmitting or remitting services is merely incidental to the actual business of the entity. Accordingly, PSPs must carefully assess whether registration as an MSB is required under the Proceeds of Crime Act on the basis of their specific business activities.

Notably, applications are also subject to a review by the Minister of Finance for reasons related to national security. The Minister of Finance may reject an application or may require undertakings or impose conditions on an applicant’s registration on national security grounds.

The BoC will also maintain a registry of registered PSPs – which will likely be similar to the registry of MSBs maintained by FINTRAC – as well as a list of persons whose registration has been refused or revoked and the reasons therefore.

## Operational Requirements

PSPs must establish, implement and maintain a risk management and incident response framework that meets certain prescribed criteria, in order to identify and mitigate operational risks and to respond to incidents. The framework will be subject to assessment by the BoC, which may provide a PSP with a list of corrective measures it considers appropriate.

## Safeguarding of Funds

Subject to exceptions for deposit-taking institutions, a PSP that holds end user funds must hold these funds in a prescribed account, a trust account that is not used for any other purpose, or an account that is not used for any other purpose and that is insured or guaranteed for at least the amount held in the account.

## Other Requirements

The RPAA will impose a mandatory notification requirement on

- a PSP that becomes aware of any incident that has a material impact on an end user, another PSP or a clearing house of a clearing and settlement system; and
- a PSP that wants to make a significant change to the way it performs a retail payment activity or add a new retail payment activity whereby the change or new activity could reasonably be expected to have a material impact on operational risk or the manner in which end user funds are safeguarded.

Registrants will also be required submit an annual report to the BoC containing information regarding their operational risk management and incident response framework and other prescribed information.

## Administration and Enforcement

The RPAA will give the BoC investigatory and audit powers, as well the power to levy administrative monetary penalties up to a maximum of \$10 million for non-compliance with the RPAA.

Notably, an individual or entity is liable for violations committed by any of its employees, third-party service providers, or agents acting in the scope of their authority, whether or not the person who actually committed the violation is identified.

## Next Steps

Currently, no date has been set for the RPAA to come into force, and the implementing regulations have not been published. Once in force, the RPAA will provide for a transitional period for PSPs to register and to conform their practices to the new requirements. Given its history and the number of open issues that remain outstanding, the RPAA is unlikely to be finalized for some time. However, PSPs in both Canada and abroad should watch the progress of the RPAA closely so they are prepared to update their practices without any interruption to their business once the RPAA comes into force.

Key Contacts: [Zain Rizvi](#), [Elliot A. Greenstone](#) and [Brian Kujavsky](#)