Regulating digital payment services: Considerations for Canadian policymakers

August 31, 2021

Advancements in contactless payment technology like “tap to pay” debit cards and Apple Pay have increased consumer demand for cashless payment methods. This demand was amplified by the COVID-19 pandemic as individuals became uncomfortable handling cash and online shopping replaced brick-and-mortar business (we discuss these trends in a four-part series).

As consumers shift away from cash and towards digital payment methods, the market for non-bank payment service providers (NBPSPs) grows. In Canada, NBPSPs have remained largely unregulated and the increasing number of NBPSPs providing bank-like services will require legislators to create a suitable regulatory regime. While the government has introduced the *Retail Payment Activities Act* (discussed here), many of the regulatory details have yet to be fleshed out.

In July 2021, the Bank for International Settlements (BIS) published, “Fintech and payments: regulating digital payment services and e-money.” The authors discuss how NBPSPs are regulated around the world, using data from a 2021 study of 75 jurisdictions. This article highlights the different regulatory schemes and could help guide Canadian policymakers as they develop the regulatory framework for digital payment services.

What are NBPSPs?

According to the BIS, NBPSPs use existing payment infrastructure, or their own standalone systems, to offer new payment methods and services to consumers. NBPSPs can be classified into two overlapping subcategories. First, those that offer storage of value in an account or device, for example, products offered by companies like PayPal. Second, those that rely on storage of value by another institution, for example, merchants and co-branded prepaid cards.

NBPSPs generally provide one or more of the following services:

- Provision of transaction accounts
- Provision of e-money transaction accounts
- Provision of electronic wallet services
- Issuing of payment instruments
- Acquiring of payment transactions
- Money or value transfer services
- Virtual asset services

- Processing of electronic funds/value transfer for third parties
- Payment initiation services
- Account information services

What is e-money?

Of the services provided by NBPSPs, e-money issuance is subject to the most intensive regulation among the jurisdictions surveyed. Interestingly, the concept of e-money isn't recognized from a regulatory perspective in Canada, where terms like "virtual currency," "cryptocurrency," "virtual assets," "digital cash," and "e-money" tend to be used interchangeably. As described by the BIS, e-money is a debt-like instrument issued on the receipt of funds for the purpose of facilitating payments. To qualify as e-money, the instrument must:

- Serve as a multipurpose medium of exchange (i.e., the instrument can be used more broadly than something like a prepaid gift card);
- Be accepted as a means of payment by parties other than the issuer; and
- Be issued only on the receipt of funds (i.e., be prepaid).

The regulatory landscape

I. Licensing and registration

Some jurisdictions have general licensing frameworks for all payment services, while others distinguish between them, e.g., licensing requirements may differ for an e-money issuer and a provider of virtual asset services. Further, some jurisdictions have distinct licensing requirements based on transaction values. For example, in Japan, payment service providers are categorized based on the maximum transaction value they can execute. The geographic area covered by the service is another basis upon which jurisdictions distinguish licensing requirements. For example, money transmitter licensing in the United States is done primarily at the state level.

In nearly all jurisdictions where non-banks are allowed to issue e-money, there are e-money-specific licensing models, namely, the narrow bank model and the non-bank model. Under the narrow bank model, non-banks can apply for a limited banking license that enables them to offer a limited set of banking services. Under this model, the licensed institutions are regulated under banking law and are therefore subject to stricter rules than traditional e-money issuers are. According to the BIS, in practice, these licenses are underused in jurisdictions where they are available, likely due to the heavy regulatory burden imposed by banking law. Under the non-bank model, specific types of non-banks are allowed to issue e-money, for example, e-money institutions, prepaid instrument issuers, or stored value issuers.

II. Minimum capital

In most jurisdictions, NBPSPs have initial and ongoing capital requirements. Typically, initial capital requirements are flat and vary depending on the payment volume permitted under the license. Alternatively, some jurisdictions' capital requirements are based on the NBPSPs location or the type of service they provide. With respect to ongoing capital requirements for e-money issuers, they are typically set as a percentage (usually 2-5%) of the e-money float.

III. Safeguarding funds security

Safeguarding requirements aim to ensure that e-money holders can redeem their e-money at face value. This can be

achieved by requiring NBPSPs to reserve assets in a commercial bank, central bank, or invest the funds in high-quality liquid assets. Safeguarding funds is required in almost all jurisdictions where non-banks are permitted to issue e-money and most jurisdictions where non-banks are permitted to provide transaction accounts.

In some jurisdictions, the safeguarded deposits are held in trust or in an escrow account so that customers' funds are segregated from the e-money issuer's and cannot be claimed by creditors in the event of bankruptcy. In other jurisdictions, this fund segregation is not required; instead, e-money issuers are required to obtain insurance. While some jurisdictions allow e-money issuers to choose any safeguarding method, others mandate a specific one.

IV. Interoperability

Interoperability is the ability for systems and software to exchange information. Pursuing interoperability aims to increase efficiency and enhance competition in the payments market. Interoperability is the least common regulatory requirement among jurisdictions. Further, its application varies widely among the types of payment services. For example, in some jurisdictions, e-money issuance requires interoperability between issuers where virtual asset services do not. Other jurisdictions have ongoing plans to achieve interoperability. The EU has adopted a new retail payments strategy with the goal that future retail payment systems are pan-European and have end-to-end interoperability.

V. Anti-money laundering/combating the financing of terrorism (AML/CFT)

AML/CFT requirements are the most common across the surveyed jurisdictions. Because NBPSPs are not subject to the same level of supervision as banks, they are seen as having higher AML/CFT risks. Generally, AML/CFT requirements include the implementation of know-your-customer (KYC) and customer due diligence (CDD) standards. Some jurisdictions apply a tiered approach to KYC and CDD, where smaller transactions have lighter regulatory requirements. A few jurisdictions go further to actually exempt certain low-risk, low-value transactions from AML/CFT requirements entirely.

VI. Consumer protection

Some jurisdictions have consumer protection laws that are specific to the financial sector or even specific to different types of payment services. Consumer protection in the context of NBPSPs focuses primarily on transparency and disclosure of information as well as dealing with customer complaints and preventing fraud.

The disclosure of information is particularly important in regards to transaction fees for money transfers. Many jurisdictions require service providers to disclose the fees charged for a transaction as well as the exchange rate margin for cross-border payments. The importance of disclosing fees was highlighted in the United Nations' 2030 Agenda for Sustainable Development in the context of reducing transaction costs for migrant remittances. In Canada, a consumer protection framework applicable to NBPSPs will have to be developed to ensure that consumers enjoy adequate protection when using new payment methods or technologies.

Conclusion

With increasing consumer demand and private sector competition in the digital payment services space, Canadian policymakers will need to find a balance between protecting consumers and promoting innovation and industry growth.

For more information reach out to Tracy Molino.

A special thank you to Caroline Harrell (articling student) for her assistance with this article.

Your Key Contacts

Tracy Molino
Counsel, Toronto
D +1 416 862 3417
tracy.molino@dentons.com