Fintech and payments: regulating digital payment services and e-money[1]

Executive summary

This paper explores how non-bank payment service providers (NBPSPs) are regulated. Improvements in technology, coupled with growing demand for digital payment methods, are increasingly reshaping the way payments are made. Covid-19 too is changing how consumers and companies purchase goods and services and make payments. While the payments space continues to be dominated by banks in many countries, the role of NBPSPs operating a variety of business models is gaining prominence. This paper provides a cross-country overview of the regulatory requirements for digital payment and e-money services offered by NBPSPs. It benefited from responses to a CPMI survey of 75 jurisdictions conducted in early 2021 and was supplemented by a desktop review of public documents issued by selected authorities.

Payment systems involve a wide range of NBPSPs. On a broad level, one can distinguish between NBPSPs that offer consumer-facing or retail services at the "front end" and those that play roles in clearing, settlement and processing at the "back end". Some NBPSPs operate closed-loop systems which combine both front-end and back-end arrangements under one roof. Among them are large technology firms – big techs – that offer payment services as part of a much wider set of activities.

The proliferation of NBPSPs in retail payments in many jurisdictions has raised questions about their regulation. The growing importance of fintech-driven NBPSPs presents opportunities. Aside from promoting financial inclusion, they could also enhance competition and efficiency in payments markets. However, this comes with potential risks in terms of consumer protection, operational and cyber resilience, the protection of funds in transit or storage, data protection, digital exclusion and market concentration. Authorities are therefore assessing whether their existing regulatory frameworks are adequate.

Among the payment services that NBPSPs can offer, e-money issuance is currently the most intensively regulated, while the provision of virtual asset services is the least. On average, jurisdictions where non-banks can issue e-money impose nine types of requirement on this service. In the case of virtual asset services, only around four types of requirement are imposed on average. Anti-money laundering (AML) and countering financing of terrorism (CFT) requirements are most commonly imposed on payment services offered by NBPSPs. Other common requirements are those relating to risk management and data protection, while the least common are those relating to interoperability. In general, this underscores that "mature" payment services tend to have well defined and fairly established regulatory frameworks but those for newer services may still be evolving. Thus, there is scope for authorities to learn more about the regulatory approaches (including the rationale for these approaches) in other jurisdictions when it comes to new payment services. This ensures that all risks arising from these services are adequately addressed in regulations.

Application of some regulatory requirements for payment services varies widely. Requirements related to AML/CFT, risk management and cybersecurity, data protection and consumer protection are, in general, uniformly applied across payment services. However, this is not the case for

[1] Codruta Boar (codruta.boar@bis.org), Johannes Ehrentraud (johannes.ehrentraud@bis.org), Aidan Lawson (Aidan.lawson@bis.org) and Jermy Prenio (jermy.prenio@bis.org), Bank for International Settlements, and Mathilde Janfils (mathilde.janfils@outlook.com), former FSI Graduate. We are grateful to Tara Rice, Committee on Payments and Market Infrastructures, and Mariam Yeghiazaryan, Central Bank of Armenia, for their involvement in earlier stages of this paper, the authorities that participated in the survey and to Patrizia Baudino, Jon Isaksen, Tanai Khiaonarong, Thomas Lammer and Alexandre Stervinou for helpful comments. Esther Künzi provided valuable administrative support.

requirements related to authorisation, minimum capital, safeguarding of funds and interoperability. The objectives of these requirements may be the same, but how they are applied across payment services can be quite different. Moreover, the practices of implementing these requirements vary significantly across jurisdictions even with the same payment service.

Non-banks can offer more types of payment service and tend to be less intensively regulated in advanced economies (AEs) than in emerging market and developing economies (EMDEs). In some jurisdictions – mostly AEs – non-banks can offer all types of payment service included in the survey, while in some EMDEs non-banks are only able to offer few. Moreover, NBPSPs in EMDEs, particularly those acquiring payment transactions, providing e-wallet services and issuing e-money, face more regulations than those in AEs. Given the potential of NBPSPs to foster financial inclusion, authorities in EMDEs might already start considering strategies for expanding their payment services markets and reviewing the appropriateness of existing regulations for these players. In this way, they can promote innovation while ensuring the safety and integrity of their financial systems.

Novel technologies are creating the potential for new means of payments to emerge. While the market capitalisation of cryptoassets is growing, it is increasingly clear that their high price volatility makes them ill-suited as a means of payment. Stablecoins, a new type of cryptoasset that emerged in 2014, are designed to maintain a stable value relative to a specified asset, or a basket of assets. While the role of stablecoins as a new payment method could potentially increase over time, the jury is still out on whether one or more stablecoins will be widely adopted as a payment method.

Regulatory approaches for stablecoins are starting to evolve. Work is under way in some jurisdictions to adapt their regulatory framework for cryptoassets, and stablecoins in particular. Prominent examples are ongoing initiatives in the United Kingdom (consultation by HM Treasury) and the United States (statement by US President's Working Group on Financial Markets, STABLE Act proposal). At present, according to a 2020 FSB survey, most jurisdictions do not have regulations that are specific to stablecoins but see the need for adjustments to existing regulations. The EU's MICA Regulation proposal, on the other hand, proposes a bespoke regulatory regime for cryptoassets including stablecoins. Absent a dedicated regulatory framework, if a stablecoin resembles an already regulated product or service, authorities will likely treat the stablecoin as such under existing regimes, which apply in whole or part depending on the coin's characteristics.

The role of big techs in payments and their potential involvement in global stablecoin (GSC) arrangements will likely receive further attention. Big techs have already captured a sizeable market share in digital payments in some jurisdictions. But even where they have not, this could change quickly due to the unique features of their business models. At present, big techs are subject to the same requirements as those of other market participants when providing financial services (including payments); and there seems to be a case for relying more on entity-based rules for big techs in certain policy areas to address the risks stemming from the different activities they perform (Carstens (2021a) and Restoy (2021)). In future, some big techs may become involved in GSC arrangements. For policymakers, it will be important to appreciate the unique combination of a very specific type of entity (big techs) providing a very specific type of activity (provision of GSC), and to consider the potential implications of this interplay.