Contents

Executive summary

Belgium hosts a number of significant financial market infrastructures (FMIs), custodians, payment service providers, such as payment institutions and electronic money institutions, as well as critical service providers and card payment processors, some of which also have a systemic relevance internationally. This Financial Market Infrastructures and Payment Services Report aims to provide a comprehensive overview of the National Bank of Belgium's oversight and supervision of these systems and institutions headquartered in, or relevant for, Belgium.

Over the last few years, several major international regulatory initiatives have been launched in the area of FMIs and payment services. In Europe, this has led to new pieces of legislation like the Payment Services Directive 2 (PSD2) and the Central Securities Depository Regulation (CSDR). The approach taken here was creating specific regulatory categories of institutions that could provide certain payment services or CSD services, setting up regulatory requirements, including the need to get licences, and the setting up of a supervisory regime.

After the phases of standard-setting and providing regulatory guidance and detailed regulatory technical standards, the regulatory emphasis has now gradually evolved to licensing institutions under these new regulatory frameworks: in 2019, under the CSDR, the NBB granted licences to two central securities depositories, and, under the PSD2, to two electronic money institutions, seven payment institutions and one payment institution providing account information services.

PSD2 and retail payments

The entry into force of PSD2, and in particular the "open banking" provisions, led to requests for licences by new types of institutions: payment initiation service providers and account information service providers. The year 2019 saw a significant increase in the number of authorised payment institutions and electronic money institutions in Belgium. This was not only due to the entry into force of PSD2 but also to UK-based payment institutions that have set up a legal entity in Belgium in anticipation of the UK's departure from the EU.

The PSD2 open banking provisions require account-servicing payment service providers (mainly banks) to open their online payment account infrastructure for access by licensed institutions (such as other banks and payment institutions). This enables these institutions to provide to their own customers payment initiation services and account information services, thereby boosting competition in the payment services market. Access to this payment accounts infrastructure is regulated with strict security requirements which must be respected by all the payment service providers concerned. The compulsory opening up of payment accounts was brought about mainly by means of a dedicated interface developed by the banks.

Another major development for underpinning innovative payment services and instruments relates to so-called faster payments. As of 4 March 2019, the Centre for Exchange and Clearing (CEC) has been able to process instant payments (retail payments that are executed within 5 seconds, even outside regular business hours and at weekends). The volumes processed are growing regularly and peaked at more than 400 000 operations per day by the end of 2019.

Cyber risks

Given the nature of their activity, operational risk is of paramount importance for FMIs and payment services providers. The NBB's oversight and prudential activities have an ongoing focus on operational resilience, including business continuity requirements. A particular area for attention is that of cyber risks. Cyber crime has been on a continuous rise over the last few years, with a significant focus on the financial sector, in particular on FMIs and payment services providers.

The NBB's oversight and supervision takes into account the importance of end-to-end security in the transaction chain, in line with the Committee on Payments and Market Infrastructures (CPMI) 2018 Strategy for reducing the risk of wholesale payment fraud related to end-point security. The SWIFT Customer Security Control Framework (CSCF), which aims to strengthen the security of the global financial community against cyber threats by providing requirements for users in terms of how they should secure their own local IT infrastructure used for connecting to SWIFT, has been analysed by overseers on the effectiveness of the implementation and reporting processes. This follow-up has included monitoring progress of adherence to and raising awareness about cyber controls under the CSCF and assisting in promotion of the framework with bank supervisors. The Bank also monitored implementation under the CSCF by institutions under its oversight work in 2019.

Internationally active FMIs and critical service providers

Belgium is home to a number of internationally active FMIs and critical service providers, such as SWIFT and Euroclear, which are also systemically relevant in other jurisdictions. In these cases, the Bank's oversight and supervision is organised through international cooperative arrangements with other central banks and/or regulators, in line with Responsibility E of the CPMI-IOSCO Principles for FMIs. Over the years, the Bank has set up processes to periodically review, and where necessary adapt, these arrangements, in order to ensure their efficiency and effectiveness, and to align them with the new regulatory frameworks, such as the CSDR.

Resilience during the COVID-19 crisis

This Report also gives an initial picture of FMIs', payment service providers' and critical service providers' resilience during the COVID-19 crisis. Most of them were well prepared to deal with extreme scenarios and could thus smoothly switch to BCP arrangements such as wide-scale home working for staff.

Pandemic recovery plans that enable FMIs to continue providing robust platforms and operations consider challenges that deviate from those encountered in more stereotypical business continuity scenarios. Unlike incidents caused by natural disasters, infrastructure failures or cyber attacks, the pandemic scenario needs to consider prolonged and potentially recurring periods of widespread operational stress. A pandemic is not a one-off incident impacting a specific location. Based on experience and the lessons learned so far, the thematic article in section 5 presents an initial overview of emerging practices for pandemic resilience.