3. Payments

The Bank has broad responsibility in the payments sphere and adopts the role of both overseer and prudential supervisor, as illustrated in chart 3 below. These approaches are complementary: while oversight concentrates on the sound and safe functioning of payment systems, payment instruments[1], payment schemes[2] or other payment infrastructures, prudential supervision aims to ensure safe, stable and secure payment service providers delivering payment services to end users.

The interest of central banks in the payments sphere stems from a connection with various core tasks. Directly or indirectly, payment systems, instruments and services may affect the practical implementation of monetary policy, the financial stability of the country, and confidence in the currency, as well as contributing to a safe, reliable and competitive environment.

Section 3.1 covers the two payment systems at the heart of the Belgian payment infrastructure: TARGET2 and the Centre for Exchange and Clearing (CEC). TARGET2 is the large-value payment system (LVPS) connecting Belgian banks with other euro area banks for processing payments and serves as the basic connecting infrastructure for the implementation of central bank monetary policy. The CEC is the domestic retail payment system (RPS) processing domestic payments between Belgian banks. In addition to TARGET2, the Mastercard Clearing Management System operated by MCE (established in Belgium) was designated as a systemically important payment system (SIPS) by an ECB Decision of 4 May 2020 pursuant to Regulation (EU) No. 795/2014 on oversight requirements for systemically important payment systems (ECB/2020/26)[3]. This Regulation lays down the – mainly quantitative – criteria which, once exceeded, lead to the designation of the entity concerned as a SIPS.

The Bank also participates in the cooperative oversight framework of CLS, a payment-versus-payment (PVP) settlement system for foreign exchange (FX) transactions. The US Federal Reserve is the lead overseer and supervisor of CLS. In addition, CLS is overseen by the Oversight Committee (OC), an international cooperative oversight arrangement comprised of the central banks whose currencies are settled in CLS and five central banks from the euro area (including the NBB).

Section 3.2 deals with the prudential supervision of payment institutions (PIs) and electronic money institutions (ELMIs) – a part of the PSP sector which offer their services in competition with the incumbent PSPs (mainly banks). This category of non-bank PSPs for retail payments provides respectively payment services and the issuing, redeeming and distributing of electronic money. ELMIs may also provide payment services and, given their ability to issue electronic money to the public, are subject to a stricter prudential regime, such as more stringent capital requirements.

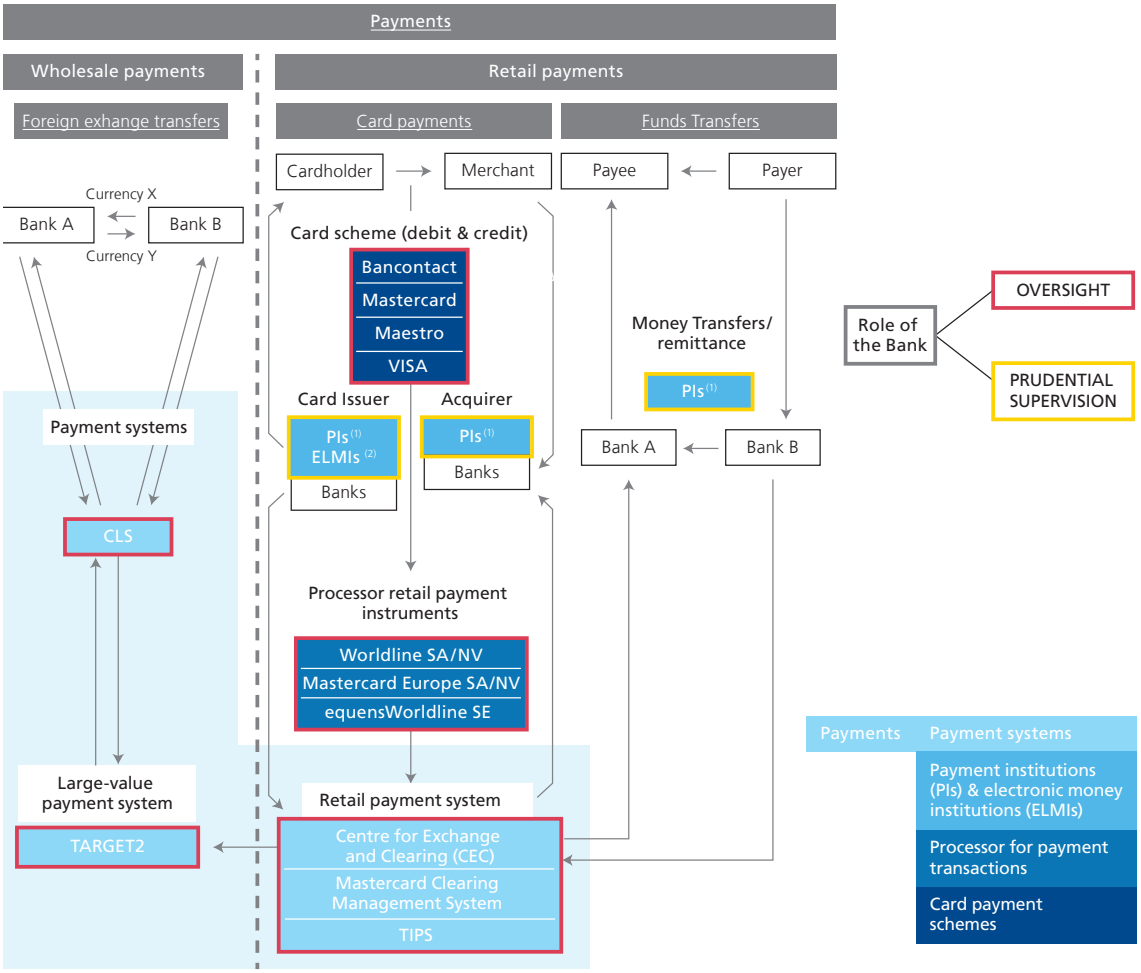
1 A payment instrument is an instrument to execute payments such as cards, credit transfers and direct debits.
2 A payment scheme is a set of rules, practices, standards and/or guidelines for the execution of payment transactions.
3 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32020D0026(01)&from=EN

As an acquirer[1] and processor of retail payment instruments in Belgium, Worldline SA/NV is subject to both prudential supervision and oversight. The Bank's activities in that respect are covered in section 3.3.

Section 3.4 covers the three payment card schemes overseen by the Bank: the domestic Bancontact scheme and the international Maestro and Mastercard schemes (these latter two being operated by Mastercard Europe SA/NV as the governance body).

Chart 3

Scope of the Bank's oversight and prudential supervision role in payments landscape



1 Payment institutions (PIs).
2 Electronic money institutions (ELMIs).

1 Acquiring card payments is a service whereby a payment service provider contracts with a payee (merchant) to accept and process payment transactions guaranteeing the transfer of funds to the payee (merchant). The processing part is often performed by another entity.

3.1 Payment systems

Changes in the regulatory framework

The Belgian and Eurosystem regulatory frameworks were not modified in 2021.

Oversight priorities / activities in 2021

Since May 2020, the Mastercard Clearing Management System (MCMS) operated by Mastercard Europe (MCE, established in Belgium) has been designated as a fourth Systemically Important Payment System (SIPS) with a pan-European reach, based on a number of mainly quantitative criteria, listed in the SIPS Regulation itself. As such, MCMS is subject to the joint lead oversight of the ECB and the NBB.

In May 2021, at the end of the initial 12-month guidance period the NBB and the ECB, with the support of a "Joint Oversight Team" (made up of representatives of the Eurosystem NCBs), started the official Eurosystem assessment of the MCMS's compliance with the SIPS Regulation. In addition to the existing reporting of incidents, more formal exchanges between the Eurosystem and MCE were initiated from the last quarter of 2021 and are intended to develop further from the early months of 2022. These exchanges involve Eurosystem officials and MCE personnel representing various governance levels and key operational functions (internal audit, risk management, change management, IT, operations & business continuity, etc.). Enhanced reporting of activities and major changes is also planned from this same period.

In 2022 the priorities will encompass the finalisation of the comprehensive assessment of compliance by the MCMS with the SIPS Regulation, which will be followed by the initiation of the assessment of MCE vis-à-vis the Cyber Resilience Oversight Expectations (CROE [1]).

The oversight activities linked to the CROE will also be performed via a joint assessment team coordinated by the NBB and the ECB, consisting of participating Eurosystem NCBs.

The CEC is the domestic retail payment system processing most of the interbank retail payments in Belgium (i.e. payments for which payer and payee use accounts in different Belgian banks). Those payments include SEPA credit transfers (SCTs), instant payments, SEPA direct debits (SDDs), card payments and the legacy of cheques. The Bank is responsible for the oversight of the CEC which takes place in the Eurosystem context on the basis of the "Revised Oversight Framework for Retail Payment Systems [2]" based on the PFMI. The CEC, which qualifies as a Prominently Important Retail Payment System (PIRPS), is compliant with the applicable standards.

In 2021, no major change was made in the CEC. However, the modifications resulting from the ECB decision on measures to increase the pan-European reach of the instant payments (IP) functionality were implemented. This mostly consisted in the migration of the technical account used for the prefunding of the IP to TIPS.

In 2022, the Bank will continue to pay specific attention to the CEC's cyber resilience.

1 The CROE are based on the guidance on cyber resilience for FMIs, which was published by the CPMI-IOSCO in June 2016. The Cyber Resilience Oversight Expectations themselves aim to provide overseers with a clear framework to assess the cyber resilience of systems and enable FMIs to enhance their cyber resilience. Unlike other sets of oversight standards applicable to payment systems (i.e. the PFMI), the CROE enable overseers to determine for each of eight specific domains which of the three maturity levels (Evolving, Advancing, Innovating) must be achieved by the systems according to their risk profiles and specific activities. The eight domains covered by the CROE are Governance, Identification, Protection, Detection, Response and Recovery, Testing, Situational Awareness, and Learning and Evolving.

2 https://www.ecb.europa.eu/pub/pdf/other/revisedoversightframeworkretailpaymentsystems201602.en.pdf

3.2 Payment Institutions and Electronic Money Institutions

Changes in the regulatory framework

Except for the developments concerning strong customer authentication and open banking (see box below), there were no changes in the regulatory framework in 2021.

BOX 6

Regulatory Technical Standards on SCA and CSC

A key mandate conferred on the EBA within the context of PSD2 relates to the drafting of regulatory technical standards on strong customer authentication (SCA) and common and secure communication standards (CSC)[1].

These RTS on SCA & CSC came into force 18 months after the entry into force of PSD2, i.e. on 14 September 2019. They form the key piece of legislation in rendering PSD2 operational in the payments landscape, as they contain both the detailed requirements on what constitutes "strong customer authentication" and any exceptions to the rule, as well as the rules on facilitating access to payment accounts for payment initiation and account information service providers.

(i) Strong Customer Authentication: fully implemented

In June 2019, the EBA published an Opinion on the elements of strong customer authentication under PSD2[2], offering the market clarifications concerning what factors may constitute inherence, possession or knowledge elements of SCA. The Opinion furthermore clarified the concepts of dynamic linking and independence of elements that are an integral part of SCA.

By the time this Opinion was issued on 21 June 2019, it had become apparent that the EBA's interpretation of the factors constituting an SCA-compliant authentication solution posed significant issues for the card payment industry.

The concerns raised by the industry were specific to online commerce (e-commerce) with payment cards. Before the summer of 2019, it became clear that the full implementation of SCA would not be achievable by the established deadline of 14 September 2019.

Strict adherence to the entry into force of the SCA requirements on 14 September 2019 could have had adverse consequences for EU customers using payment cards in online commerce. It was considered

1 Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication (hereafter: RTS on SCA & CSC).

2 EBA Opinion 2019_06 on the elements of strong customer authentication under PSD2, 21 June 2019.

paramount by regulators across the EU that customers would continue to be able to make payments, including online, with payment cards, without suffering interruptions.

In response to industry concerns, the EBA's aforementioned Opinion provided the option to each competent authority (CA) under PSD2 "*on an exceptional basis and in order to avoid unintended negative consequences for some payment service users after 14 September 2019, to work with PSPs and relevant stakeholders, including consumers and merchants, to provide limited additional time to allow issuers to migrate to authentication approaches that are compliant with SCA, and acquirers to migrate their merchants to solutions that support SCA*".

The EBA further specified that this supervisory flexibility is conditional upon PSPs setting up a migration plan, agreeing the plan with their CA, and executing the plan as quickly as possible. CAs should also monitor execution of these plans to ensure swift compliance with PSD2 and the EBA's technical standards, and to achieve consistency of authentication approaches across the EU.

As described in the previous Report, over the 2019 summer period the Bank conducted an analysis of the state of readiness of the Belgian market based on which, on 28 August 2019, the Bank took advantage of the supervisory flexibility option provided by the EBA. This resulted in the publication in early May 2020 of the Belgian roadmap for this migration.[1]

In October 2019 the EBA published an Opinion on the deadline for the migration to SCA for e-commerce card-based payment transactions[2], effectively aimed at harmonising the deadline for supervisory flexibility by CAs in order to avoid divergent end dates for compliance with the SCA requirements. The EBA established this end date at 31 December 2020 and the Bank adhered to it in 2020.

By the end of the year it had become evident that quite a few Member States would not be in a position to migrate to full SCA compliance for their card industry by the 31 December 2020 deadline. Given the highly cross-border nature of Belgian Visa, Mastercard and American Express online card transactions (owing to the very cross-border nature of e-commerce), it would have been detrimental for Belgian cardholders to have their card transactions denied if Belgian banks could not allow payments without SCA to go through on the websites of commonly used foreign merchants based in neighbouring countries in the EEA. At the same time, not all Belgian merchants were ready to process SCA-compliant transactions on their websites by the end of the year.

In order to align itself with neighbouring countries and to avoid disruption to online commerce during the festive season, at a time when Covid-19 was limiting in-store purchases, the Bank granted the industry an additional reprieve, adapting the planned timeline for full compliance by moving the ultimate deadline to mid-May 2021. By 18 May 2021, full compliance with SCA requirements was achieved for online card transactions. This timing was similar to that in neighbouring countries and ensured a smooth transition without disrupting Belgian cardholder transactions with both Belgian and foreign merchants.

1 Available at https://www.nbb.be/doc/cp/eng/2020/belgian_roadmap_sca.pdf

2 EBA Opinion 2019_11 on the deadline for the migration to SCA for e-commerce card-based payment transactions, 16 October 2019, available at https://www.eba.europa.eu/eba-publishes-opinion-on-the-deadline-and-process-for-completing-the-migration-to-strong-customer-authentication-sca-for-e-commerce-card-based-payment

It should also be noted that SCA is required not only for card payment authentication but whenever payers (i) access their payment account online; (ii) initiate an electronic payment transaction (irrespective of the underlying payment instrument), or (iii) carry out any action through a remote channel which may imply a risk of payment fraud or other abuses. Since 14 September 2019, the Bank has therefore also been tasked with monitoring compliance with the SCA requirements by all PSPs concerned, including in the online banking environment.

(ii) Open banking: access to payment accounts

A second key part of the RTS on SCA & CSC sets out common and secure communication standards (CSC) for communication between account servicing payment service providers (ASPSPs) and payment initiation and account information service providers (collectively referred to as third-party providers or TPPs). These requirements detail how ASPSPs should provide access to their payment accounts to TPPs in a secured fashion.

The RTS on SCA & CSC provides two ways in which ASPSPs can arrange access for TPPs to their online available payment accounts: (i) establishment of a dedicated interface; or (ii) use of an adapted customer interface. Each ASPSP has the choice between a dedicated or an adapted customer interface. In Belgium, almost all ASPSPs have opted for a dedicated interface.

On 4 June 2020, the EBA published an Opinion on the obstacles to the provision of TPPs' services under the RTS on SCA and CSC[1]. The Opinion aims to support the PSD2's objectives of enabling customers to use new and innovative payment services offered by TPPs, namely by addressing a number of issues regarding the interfaces provided by ASPSPs to TPPs. It clarifies several obstacles identified in the market, including requiring multiple SCAs, the manual entry of the IBAN in the ASPSPs' domain, or imposing additional checks on the consent given by the customer to the TPP. In a follow-up Communication, the Bank confirmed that it shares the stated view of the EBA and will integrate the Opinion into its supervisory approach. The Bank nonetheless acknowledged in its statement that implementation of the required technical changes to the interfaces takes time. In view of this, the Bank confirmed that it expected the sector to comply with this Opinion by 31 December 2020 at the latest.

The Bank conducted detailed assessments of each dedicated interface offered by ASPSPs under its supervision in the first months of 2021 in order to assess whether the stated deadline had been adhered to. Unfortunately, this yielded a mixed picture, demonstrating that some ASPSPs in our market continued to be non-compliant with certain key elements of the aforementioned EBA Opinion. The Bank wrote to each of these ASPSPs individually in the spring of 2021, giving them formal notice for these key elements and admonishing them to render their dedicated interface(s) compliant with these specific legal requirements within a certain timeframe or face potential repercussions under prudential law. A second in-depth review of each dedicated interface in September and October 2021 demonstrated significant progress by APSPs in this domain. Almost all these key issues related to compliance with the aforementioned EBA Opinion have been solved by the end of 2021.

1 EBA Opinion 2020_10 on obstacles under Article 32(3) of the RTS on SCA and CSC, available at https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Opinions/2020/884569/EBA%20Opinion%20on%20obstacles%20under%20Art.%2032%283%29%20RTS%20on%20SCA%26CSC.pdf

Looking ahead to 2022, the Bank continues to monitor both the continuing clarification of the legal framework under PSD2 related to access to payment accounts, and the situation regarding dedicated interfaces in our country. To that end, the Bank anticipates having to further clarify its position on some aspects pertaining to this legal framework and subsequently ensuring their consistent implementation by ASPSPs under its supervision.

Ongoing prudential supervision in 2021 and priorities in 2022

The Bank's main supervisory activities in 2021 still consisted primarily of i) the authorisation of new payment institutions, electronic money institutions, registration of limited networks and ii) monitoring the implementation of the requirements related to the RTS on strong customer authentication and common and secure communication within the Belgian market. In addition, i) specific attention was paid to the safeguarding requirements of funds received by payment and electronic money institutions from payment service users, leading to an extension of the periodic reporting, and ii) in 2021 the Bank launched a cross-sectional analysis of the IT security policies.

In 2022 the Bank intends to take a closer look at i) the outsourcing of important operational functions, and ii) the results of the new reporting on the safeguarding of funds; it also intends to iii) continue the cross-sectional analysis of the IT security policies, iv) monitor the SCA compliance and the potential open banking obstacles, and v) follow up the implementation of changes in Belgian company law.

Over the past year three institutions[1] were granted a licence, one of which (Batopin N.V.) will probably become a significant market infrastructure in terms of cash distribution, and three institutions[2] were withdrawn from the official lists. Consequently, the number of institutions remains stable at 40 compared to last year. Including the European branches, Belgium has 47 payment institutions and electronic money institutions. On a very regular basis, the Bank is contacted by new candidates with existing or new business models, which indicates that the number of institutions will increase in the coming year.

With regard to the business models of new service providers, in 2020 the Bank observed the collaboration between traditional banks or financial institutions and up-and-coming fintech players. This trend has intensified over the past year. In a quest for profitability, the account information service providers and payment initiation service providers seek further cooperation with traditional banks, other financial institutions and corporates active in the accountancy and document handling market.

In the past year, the Bank noted that some Belgian banks or financial institutions ended their cooperation with payment institutions offering money remittance services. As a result, these institutions had to look for alternatives.

1 Tap Tap Send, Batopin and Augias Corp.
2 HiPay ME, Airplus International and Travelex.

3.3 Payment transaction processors

Changes in the regulatory framework

In 2021, there were no changes in the Belgian regulatory framework applicable to payment transaction processors.

Prudential & oversight approach

In 2021, no new entity providing processing services in the Belgian payments market was designated as a systemically important payment processor. Table 3 shows the entities that have the status of systemically important processor of payment transactions based on Article 6 of the Law of 24 March 2017 on the oversight of payment transactions processors and the scheme(s) for which they have such status.

Table 3

List of systemically relevant payment processors

(as at 31 December 2021)

Systemically relevant payment processors	Payment scheme for which the legal threshold is exceeded	
	Bancontact	Maestro
Worldline NV/SA	✓	×
equensWorldline SE	✓	✓
Mastercard Europe SA	×	✓

Source : NBB.

Systemically important processors must comply with requirements that aim to maintain the stability and continuity of retail payments in Belgium, e.g. the obligatory comprehensive risk management in the fields of detection, appraisal and development of mitigation measures. The legal framework for payment transaction processors also includes a strict process for incident reporting to the Bank, and enables the latter to apply a sanctions regime. The Bank's oversight of such processors focuses on cyber resilience and operational reliability.

3.4 Card payment schemes (CPS)

Regulatory framework

In November 2021, the Eurosystem published a new oversight framework designed to foster improvements in the soundness and efficiency of electronic payments. This new oversight framework for electronic payment instruments, schemes, and arrangements (PISA Oversight framework) is based on the internationally agreed Principles for Financial Market Infrastructures (PFMI). It is now the benchmark for Eurosystem oversight of

payment instruments, schemes and arrangements, and replaces the former standards used by the Eurosystem[1]. The PISA oversight framework was designed with the objective of addressing technological developments in the payment industry. The framework[2] itself is complemented by an assessment methodology[3] and an exemption policy[4]. This policy aims at identifying schemes and arrangements of a certain importance and level of risk based on specific criteria relating to the size of the user population, market penetration in terms of value and volume, and geographic relevance. Only those schemes and arrangements will have to comply with the requirements of the framework. In Belgium, this concerns Mastercard Europe and Bancontact. Like all companies that are already subject to Eurosystem oversight, both card payment schemes are expected to adhere to the principles of the new framework by 15 November 2022.

Oversight priorities / activities in 2021

The Belgian domestic CPS, Bancontact, is subject to oversight by the Bank. In 2022 the Bank will direct its attention towards the scheme's compliance with the PISA oversight framework. Bancontact will be invited to submit self-assessments and supporting documentation. This will form the basis of a dialogue aimed at assessing compliance with the PISA framework.

For MCE, which qualifies both as a CPS and as a SIPS, and with a view to avoiding duplication of tasks, the new PISA framework provides for account to be taken of the results of every oversight duty performed during the monitoring of its continuous compliance, as a SIPS (see section 3.1), with the requirements of the SIPS Regulation.

The Regulation on interchange fees for card-based payment transactions (IFR) encompasses a specific requirement on the unbundling of scheme and processing activities within the same legal entity as regards the accounting, organisation and decision-making processes, which is also applicable to MCE and Visa Europe. In this context the Bank is the leading National Competent Authority (NCA) in charge of the coordination of the working group devoted to MCE. In its capacity as the NCA for MCE, the Bank has shared its provisional analysis with the cooperative working group members. The latter issued a number of attention points and clarification requests which were subsequently addressed by MCE and then further assessed by the Bank. A final report analysing MCE's compliance with IFR Article 7.1.a should be completed by the end of the first quarter of 2022.

1 These standards include:
- The harmonised oversight approach and oversight standards for payment instruments (ECB, February 2009);
- The oversight framework for card payment schemes (ECB, January 2008);
- The oversight framework for direct debit schemes (ECB, October 2010);
- The oversight framework for credit transfer schemes (ECB, October 2010);
- The "Electronic money system security objectives" (ECB, May 2003),

2 Available at https://www.ecb.europa.eu/paym/pdf/consultations/ecb.PISApublicconsultation202111_1.en.pdf

3 Available at https://www.ecb.europa.eu/paym/pdf/consultations/ecb.PISApublicconsultation202111_2.en.pdf

4 Available at https://www.ecb.europa.eu/paym/pdf/consultations/ecb.PISApublicconsultation202111_3.en.pdf