3. Payments

The Bank has broad responsibility in the area of payments 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 pursues safe, stable and secure payment service providers delivering payment services to end users.

The interest of central banks in the area of payments 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, confidence in the currency, as well as contribute to a safe, reliable and competitive environment.

Section 3.1 covers the two payment systems which are core for 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 criteria, mainly of a quantitative nature, which, once exceeded, lead to the designation of the concerned entity 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 PSP's (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 stronger capital requirements.

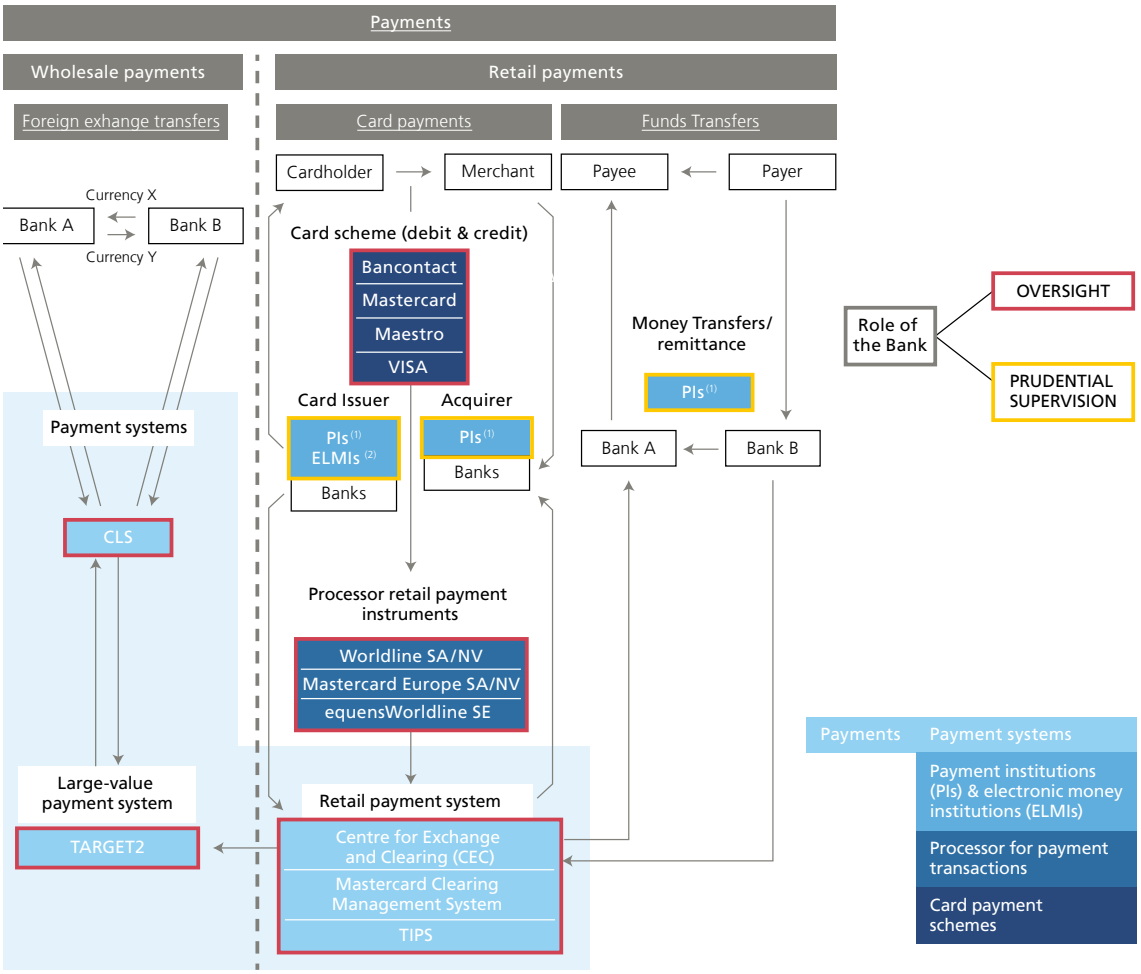
As acquirer[4] and processor of retail payment instruments in Belgium, Worldline SA/NV is subject to both prudential supervision and oversight. The Bank's activities in that respect are covered in section 3.3.

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/?uri=CELEX%3A52020XB0026.
4 Acquiring card payments is a service whereby a payment service provider contracts with a payee (merchant) to accept and process payment transactions guarantying the transfer of funds to the payee (merchant). The processing part is often performed by another entity.

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 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).

BOX 6

The European Commission, the European Central Bank and the NBB unfold their retail payments strategies

The Bank and international regulators have gone through an update of their key priorities in the retail payments area.

In connection with its digital finance strategy, the EC[1] developed a specific retail payments strategy for Europe focusing on four key pillars, which are closely interlinked: 1) increasingly digital and instant payment solutions with pan-European reach; 2) innovative and competitive retail payments markets; 3) efficient and interoperable retail payment systems and other support infrastructures; and 4) efficient international payments, including remittances.

The key objectives laid out in the EC's retail payments consultation were aligned with the Eurosystem's retail payments strategy adopted by the **ECB**'s Governing Council with its main goal to support and foster development of pan-European Point Of Interaction (physical Point Of Sale – POS – + e-commerce) payment solutions. Other major goals consist of a full deployment of instant payments, support for innovation and an innovative payments ecosystem, an improvement of cross-border payments as well as work on eID/eSignature.

At the national, Belgian, level, **the Bank** plays an important role in fostering the modernisation of payment services in order to meet the public policy objectives of safety, efficiency, availability and meeting end-user needs and expectations. The Bank conducted a thorough strategic exercise and concluded on its policy stance on various topics which are aligned with the international regulators' views.

The main action point of the Bank's strategic exercise was to establish a new committee to bring together all the parties involved at the highest level with the aim of ensuring that its policy objectives are ensured under the best possible conditions in Belgium. This **National Retail Payments Committee (NRPC)** is chaired by NBB Director Tim Hermans and members include all relevant stakeholders in the area of the retail payment ecosystem:

- public sector representatives (public institutions in the domains of Finance, Consumer Protection, Economy, Administrative Simplification, Treasury);
- corporate and retail sector representatives;
- consumer representatives;
- representatives of the financial sector entities active in retail payment services (credit institutions, payment and electronic money institutions);
- Belgian financial market infrastructures (FMIs), payment schemes and systemic operators in the field of payments;
- transport sector for cash (CIT, Cash-In-Transit);
- other supervisors/regulating bodies.

1 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a Retail Payments Strategy for the EU (COM/2020/592 Brussels, 24.9.2020).

The Bank is well placed to initiate this, since its powers cover all means of payment, the payment systems/schemes and payment services. The core objective of the NRPC is to facilitate discussion and consultation relating to retail payments in Belgium in order to enable the smooth functioning of the Belgian economy, taking account of public interest considerations. Inefficiencies in the retail payments market may actually have significant negative effects throughout the economy.

By discussing and consulting within the NRPC community, all relevant stakeholders are expected to apply the collective knowledge, experience, and ability to gain a more complete understanding of the retail payment ecosystem. Using this knowledge, members can individually and unilaterally make appropriate decisions regarding their own business risks and opportunities.

The NRPC potentially handles the following non-exhaustive list of topics:

- safe and efficient payment services/activities/instruments and access for domestic and cross-border purposes;
- availability and accessibility of cash;
- acceptance of cash;
- security, transparency and awareness regarding the usage of payment instruments;
- discussion and monitoring of technological developments;
- update on regulatory developments;
- monitoring trends in retail payment activities.

It is the Committee's policy to govern its activities in compliance with the applicable competition laws at all times.

3.1 Payment systems

Changes in regulatory framework

The Belgian and the Eurosystem regulatory frameworks applicable to payment systems were not changed at all in 2020.

Oversight approach

With the ECB as the lead overseer, the Eurosystem is responsible for oversight of three Systemically Important Payments Systems (SIPS): TARGET2, EURO1 and STEP2. They are overseen on a cooperative basis along with the national central banks in the Eurosystem.

As from May 2020, the Mastercard Clearing Management System (MCMS) operated by MCE (established in Belgium) has been designated as a fourth SIPS with a pan-European reach (while the fifth SIPS has full national anchorage). The activities of MCE as a SIPS stem exclusively from the card-based transactions under the debit and credit card schemes managed by MCE. The combination of this pan-European reach with this strong link to the MCE's scheme activities for which the NBB was the lead overseer since 2008, have led the Eurosystem to appoint both the ECB and the NBB as joint competent authorities for the oversight of this system. The designation of

MCMS as a SIPS stems from MCE fulfilling a number of criteria, listed in the SIPS Regulation itself and mainly of a quantitative nature, referring to market shares, cross-border activities.

The Bank is responsible for the oversight of the CEC, the Belgian domestic retail payment system. The last major change in the system was the launch, on 4 March 2019, of a platform for the processing of instant payments (IP) which was integrated into the existing automated clearing house as an additional functionality. In 2020, the Bank continued to monitor the functioning of the CEC and particularly the IP functionality. No significant incident was observed. Almost 100 million IP operations were processed in 2020 (which represents about 15 % of all credit transfers processed by the system) with daily peaks at more than 500 000 operations.

Supervisory priorities in 2021

Regarding the Mastercard Clearing Management System, the 12-month period following its 4 May 2020 designation as a SIPS, were to be considered as a grace period. Along the latter the NBB and the ECB, with the support of a "joint oversight team" (made up of representatives of the Eurosystem NCBs), have provided support to MCE efforts with a view to render its SIPS compliant with the SIPS Regulation at the May 2021 horizon. The effective official assessment by the Eurosystem of the MCMS compliance has started in May 2021 and is expected to last about one year. As from the same May 2021 milestone, an extended reporting will be expected from MCE as the operator of the MCMS, in terms of activities, incidents and major changes. This SIPS qualification will also entail a set of more formal exchanges between the Eurosystem and representatives of different governance levels and key operational functions (risk management, IT, internal audit, operations & business continuity, change management, etc.) of MCE.

In 2021, the Bank will continue to pay specific attention to the development of the CEC's cyber resilience as well as, for the IP functionality, to the implementation modifications resulting from the ECB Decision on measures to increase the pan-European reach of instant payments.

3.2 Payment Institutions and Electronic Money Institutions

Changes in regulatory framework

In 2018, the second Payment Services Directive 2015/2366 (PSD2)[1] was transposed into Belgian legislation. PSD2 aims to encourage innovation and competition by enabling new players to offer new types of payment services on the market. The Directive also aims for simpler, safer and more efficient payment transactions within Europe through such things as the introduction of the concept of strong customer authentication.

PSD2 was transposed into Belgian law via two pieces of legislation. The first one, the Law of 11 March 2018[2], contains the prudential aspects of PSD2 and falls within the competence of the Bank. This Law also repeals and replaces the Law of 21 December 2009. The second piece of legislation, the Law of 30 July 2018 amending Book VII of the Code of Economic Law, contains consumer protection and conduct of business rules and falls within the competence of the Federal Public Service Economy.

1 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No. 1093/2010, and repealing Directive 2007/64/EC, OJ. 23 December 2015, L 337, 35-127.

2 The Law of 11 March 2018 on the legal status and supervision of payment institutions and electronic money institutions, access to the payment service provider's business and the issuing of electronic money activity, and access to payment systems.

In 2019, the last Royal Decree[1] within the framework of the Law of 11 March 2018 was issued. This Royal Decree stipulates the regulations of the Bank on own funds requirements for electronic money institutions. More specific, the Decree requires that the prudential own funds of electronic money institutions must at any time be at least equal to the maximum of €350 000 or the sum of the required equity calculated on the basis of the issued electronic money, which equals to 2 % of the average outstanding money, and the provided payment services, for which the regulatory framework defines three different methods (A, B or C).

In order to develop a coherent legal framework at Community level, the European Commission also conferred 12 mandates on the EBA within PSD2. These mandates consist of five RTSs[2] (Regulatory Technical Standards), which are of direct effect across the European Economic Area, and 7 Guidelines, which were implemented in the Bank's supervisory framework via Circulars issued in 2018 and 2019. An important element of the Law of 11 March 2018 relates to the requirement for institutions to remain responsible for the fulfilment of all its obligations of its outsourced functions, activities or operational tasks. In particular, outsourcing may not lead to the quality of internal control being compromised, nor to any unnecessary increase in operational risk.

In line with this, the EBA issued a set of guidelines on outsourcing on 25 February 2019. These were implemented in Belgium by the Circular of 19 July 2019[3], which is also applicable to payment institutions and electronic money institutions. The Circular sets out a transitional period for existing outsourcing agreements until 31 December 2021 and requires institutions to report the following to the Bank : i) an outsourcing register, ii) planned outsourcing of critical/important functions, iii) a notification when outsourced functions become critical/important and iv) a notification when there are material changes or critical incidents concerning outsourcing agreements.

In an amendment to its 2018 guidelines, the EBA updated the guidelines on fraud reporting under PSD2 on 22 January 2020. The Circular of 24 March 2020[4] reflects these changes, which are mainly technical in nature. In addition, further EBA guidelines on ICT and security risk management were transposed by way of the Circular of 16 June 2020[5], which requires all payment and electronic money institutions to report on any operational and security risks as well as applicable mitigating measures. In order to capture the significant changes over the years, the framework Circular was replaced by the Circular of 8 July 2020[6] concerning the prudential statute of payment institutions and electronic money institutions. This Circular gives an overarching overview of the legal framework that applies to payment and electronic money institutions.

1 Royal Decree of 21 March 2019 approving the rules of the National Bank of Belgium on own fund requirements of electronic money institutions.
2 The RTS on home-host cooperation has been adopted by the EBA and been submitted to the European Commission. The final RTS still needs to be published by the European Commission.
3 Circular 2019_19 on the guidelines of the European Banking Authority of 25 February 2019 on outsourcing.
4 Circular 2020_007 on the guidelines of the European Banking Authority of 22 January 2020 on fraud reporting under PSD2.
5 Circular 2020_24 on the guidelines of the European Banking Authority of 29 November 2019 on ICT and security risk management.
6 Circular 2020_27 on the prudential statute of payment institutions and electronic money institutions.

BOX 7

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. It forms the key piece of legislation in rendering PSD2 operational in the payments landscape as it contains both the detailed requirements on what constitutes "strong customer authentication" and any exceptions to the rule, as well as the rules on rendering access to payment accounts possible for payment initiation and account information service providers.

(i) Strong Customer Authentication: ongoing work

As mentioned in the 2020 FMI and Payment Services Report, in June 2019, the EBA published an Opinion on the elements of strong customer authentication under PSD2 in which clarifications were provided to the market concerning what factors may constitute inherence, possession or knowledge elements of SCA. This 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 handed down on 21 June 2019, it had become apparent that the EBA's interpretation of which factors constitute an authentication solution that may be considered as SCA posed significant issues for the card payment industry. The concerns raised by the industry were specific to online commerce (e-commerce) with payment cards.

The first concern related to authentication solutions for payment cards in online commerce being based on non-SCA compliant use of the card details (as printed on the payment card). The second concern related to the technical capabilities in the industry to make use of the nine exceptions to the rule of strong customer authentication listed in the RTS on SCA & CSC. These exceptions were purposefully crafted in order to ensure the smooth working of electronic payments, including online commerce with payment cards. Examples include the use of contactless payments at a point of sale under a certain amount in euro, low-value transactions and transaction risk analysis when the fraud rates are sufficiently low. However, in order to render the use of these exceptions operational in the sphere of online commerce with payment cards, it requires smooth communication of the desire to leverage a particular exception between online merchants' websites, their payment card acquirers and the issuers of those payment cards. The communication protocol best suited to establish this communication is often referred to as EMV 3DS.

In response to these two 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

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).

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".

As the reader may recall, the Bank leveraged on 28 August 2019 this supervisory flexibility option provided by the EBA which resulted in the first half of 2020 in the approval of a roadmap for this migration agreed between the involved stakeholders and published on the Bank's website in early May 2020[1].

Apart from mitigating the two concerns stated above, a key strategy of this migration plan is to migrate incrementally towards full SCA compliance for all card transactions through the use of a mechanism of soft declines whereby a card transaction that is not strongly authenticated is returned to the merchant for authentication providing the merchant with an opportunity to strongly authenticate the cardholder instead of being confronted immediately with a declined card transaction. By incrementally increasing the threshold underneath which this soft decline is applied, the migration plan ensures a gradual uptake of SCA requirements providing the card payment industry, and importantly, e-commerce merchants with ample time to adjust as well as identify and solve any problems that may arise on a technical level.

Following publication of the migration plan in early May 2020, the Bank has actively been monitoring the ongoing march towards a successful implementation of SCA for the online card environment. During the course of 2020, the first concern stated above has been fully mitigated by payment service providers under supervision of the Bank. In relation to the second concern, Belgian payment service providers (issuers and acquirers) have achieved a high level of implementation of the required communication protocol EMV 3DS. It should nevertheless be noted that payment service providers are heavily dependent to a large degree on e-merchant websites (both domestic and – even more so – foreign) making the necessary technical implementations in order to render SCA-compliant card transactions possible on their websites and in their mobile applications.

In supervising the phased roll-out of SCA for these card transactions, the Bank pays special attention to the situation in neighbouring countries with which Belgian cardholders interact frequently in the field of e-commerce. Taking into account the impact of the COVID-19 pandemic on the importance of e-commerce for Belgian cardholders and of not disrupting e-commerce, the Bank therefore seeks to avoid unnecessary friction in the online e-commerce market for Belgian cardholders. Accordingly, the Bank has sought and continues to seek to ensure a high level of alignment, wherever and whenever feasible, with neighbouring markets in supervising and enforcing SCA for the e-commerce card industry. The current state of the SCA migration plan reflects this endeavour.

It should furthermore 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. The Bank is therefore also tasked with monitoring compliance with the SCA requirements by all PSPs concerned since 14 September 2019, including in the online banking environment.

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

(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 avenues for ASPSPs towards establishing access for TPPs to their online available payment accounts: (i) establishment of a dedicated interface; or (ii) use of an adapted customer interface. The choice between dedicated or adapted customer interface is to be made by each ASPSP. In Belgium, almost all ASPSPs have opted for the use of a dedicated interface. When an ASPSP opts for a dedicated interface, it must provide a contingency mechanism in case its dedicated interface fails. Provided this dedicated interface meets certain requirements, it can be exempted from the requirement to foresee a contingency mechanism.

The establishment of fully functional dedicated interfaces by Belgian ASPSPs has not been without effort. For credit institutions that provide multiple payment services (e.g. single SCT, batch payments, standing orders, future-dated payments, instant payments, etc.) across multiple online channels (mobile and website) and multiple customer segments (retail, corporate, SME, etc.), the roll-out of a set of APIs that together constitute the dedicated interface providing access to TPPs to all these payment functionalities for all payment accounts of all customers is a technically complex and lengthy process that did not end abruptly in September 2019 but is rather incrementally continuing as new versions of the dedicated interface are brought into production.

On 4 June 2020, the EBA published an Opinion on the obstacles to the provision of TPPs under the RTS on SCA and CSC. The Opinion clarifies a number of obstacles identified in the market, including requiring multiple SCAs, the manual entry of the International Bank Account Number (IBAN) in the ASPSPs' domain, or imposing additional checks on the consent given by the customer to the TPP. The Bank confirmed that it shares the stated view of the EBA and integrated 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 have complied with this Opinion by 31 December 2020 at the latest. This deadline was shared by the majority of national competent authorities (NCAs) in the European Economic Area (EEA).

Throughout 2020, as in 2019, the Bank engaged proactively with Belgian ASPSPs in order to clarify the relevant legal framework and its interpretation.

To assess the individual readiness of each ASPSP with the end-of-2020 deadline, the Bank sent out questionnaires to all concerned ASPSPs in the third quarter of that year. From the responses and subsequent bilateral meetings held with ASPSPs, it could be concluded that several obstacles in dedicated interfaces were prevalent at that time. These include, among other things, lack of support for all payment functionalities (e.g. instant payments, bulk/file payment and international payments), lack of incorporation of certain authentication procedures (e.g. face/fingerprint recognition, Itsme), lack of implementation of an app-to-app and web-to-app redirection with as a consequence that certain payments cannot be executed and/or certain functionalities are off-limits to TPPs dependent on the

channel in which the TPP is active (mobile or web), the failure to implement a contingency mechanism if the dedicated interface is not exempted from it and the existence of other obstacles as listed in the aforementioned Opinion, e.g. requiring multiple SCAs in the redirection flow, rendering account selection difficult, verifying payment service user consent at ASPSP level and requesting additional TPP registrations.

The Bank emphasised to ASPSPs that the deadline had to be met and obstacles should have been removed by 31 December 2020. The Bank continues to prioritise the verification and monitoring of the removal of all obstacles as listed above from dedicated interfaces in order to ensure that continued non-compliance does not prevent TPPs in Belgium from offering RTS-compliant payment initiation and account information services and to ensure a level playing field among and equal treatment between compliant and non-compliant ASPSPs. In cases of continued non-compliance, the Bank may have to consider what steps would be most appropriate to mitigate the situation.

Supervisory Priorities in 2020 and 2021

The Bank's main supervisory activities in 2020 consisted primarily of i) authorisation of new payment institutions, electronic money institutions and registration of limited networks, ii) monitoring implementation of the requirements related to the RTS on strong customer authentication and common and secure communication within the Belgian market[1] and iii) completing the final changes to the prudential supervision model as set out in PSD2.

The number of payment institutions/electronic money institutions under supervision has risen over the past year from 31 to 37[2], led by a notable increase in firms, both start-ups and incumbents, wishing to apply for the required authorisation to be able to provide payment initiation and account information services. Institutions offering money remittance services have also expressed significant interest. This could be explained as a result of Brexit and the expiry of the transition measures, leading many enterprises to finalise their move to the European Union in order to continue providing their respective services. The number of electronic payment institutions remained stable with seven institutions under supervision in 2020.

Within this context, the Bank observes the following trends with regards to the business models of new service providers:

- collaboration between traditional banks and financial institutions with up-and-coming FinTech players;
- consolidation of specialised payment providers in the card payments sector;
- continued interest in the provision and issuance of crypto-currency and assorted services.

Regarding the first trend, the Bank has observed that a growing number of banks have partnered or acquired FinTech enterprises providing account information and payment initiation services. Even as the possibilities of open banking are unfolding, the landscape is highly fragmented and has ample opportunities for consolidation, a trend which is seen in Belgium and the rest of the European Union.

1 See Box 7.
2 33 Reasons, Jubilee Services, Sendwave, GuiSquare, Together Connected, PagoFX.

The second observed trend relates to the increase in consolidations across Belgian card payment providers, more specifically expense cards. Following the entry into force of the Interchange Fee Regulation (IFR), caps have been imposed on consumer debit and credit cards, leading to lower profitability for providers. In order to deal with mounting costs, mainly in terms of processing, mergers in the sector seek to restore profitability.

Recent activity in crypto-markets as well as regulatory developments within the EU have fuelled a barrage of questions regarding crypto-currencies. In the absence of common European legislation, whereby some countries[1] have implemented national solutions, uncertainty remains rife. So, the provision or use of crypto-services is exposed to significant risks for enterprises and consumers alike. As a matter of policy, the Bank takes a prudent stance towards the offering of crypto-assets in Belgium while awaiting the MiCA framework (see thematic article) to which it contributes to via the appropriate regulators' fora.

In the coming year, several of the recently implemented changes will be expanded upon. The installation of a team of inspectors has allowed the Bank to organise an in-depth review of asset segregation among regulated payment institutions and institutions for electronic money. New reporting requirements will also support a scale-up of regulatory supervision, including in new areas such as (critical) outsourcing, which will be reported on for the first time by all regulated entities.

Concerning the monitoring of implementation of the requirements related to the RTS on strong customer authentication and common and secure communication, specific focus will be laid on both the migration plan for SCA in online commerce with payment cards and the roll-out of dedicated interfaces in Belgium, which would foster full deployment of payment initiation and account information services within the market.

For SCA, the focus will be on ensuring that the migration plan continues to be followed by all domestic market participants. The Bank will at the same time continue its ongoing monitoring of SCA compliance across all payment service providers in the market.

For access to payment accounts, the focus will be on actively monitoring adherence by ASPSPs to the 31 December 2020 deadline and the effective removal of remaining obstacles in 2021 in order to ensure the creation of stable and fully functional dedicated interfaces enabling the provision of TPP services in the Belgian market.

The continued transformation of the payments market, combined with further developments related to open banking, will show whether new service providers can develop a sustainable business model and obtain a permanent and stable stake within the payments landscape. The Bank will therefore actively monitor developments taking place within this context.

1 Such as Germany and France.

BOX 8

Money remittance in Belgium

Money remittance is a long-established payment service regulated in Europe by the second Payment Services Directive (PSD2), where funds are received from a payer, without any payment accounts being created in the name of the payer or the payee, for the sole purpose of transferring a corresponding amount to a payee or to another payment service provider acting on behalf of the payee, and/or where such funds are received on behalf of and made available to the payee. Remittances are playing an increasingly large role in the economies of small and developing countries.

In 2019, two money remittance companies were granted a licence by the Bank, and two more in 2020 At the end of 2020, nine money remittance companies were listed as a Belgian payment institution. The Belgian payment institutions have an agent network of 253 agents in Belgium and 8 312 agents[1] in other EEA countries, an increase of 4 %. In addition to the 253 Belgian agents, 1 586 agents of other European payment institutions are active in Belgium.

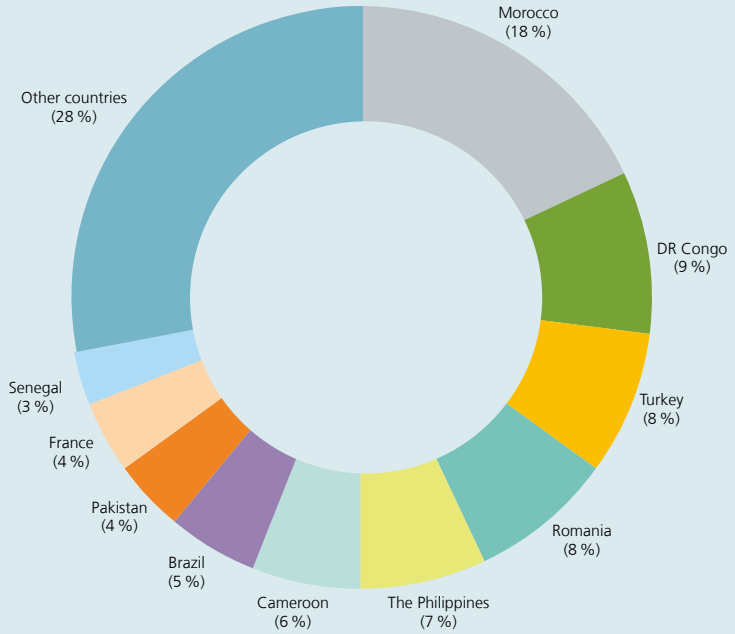
1 91.3 % of the agents work on behalf of Moneygram International, which re-located from the UK to Belgium at the end of 2017, because of Brexit.

Overview of money remittance in Belgium

Money transfers by all money remitters present in Belgium

(2019, yearly total, payment institutions established in Belgium or other EEA Member States)

Chart – Top-10 Country Corridors in value IN & OUT money transfer flows

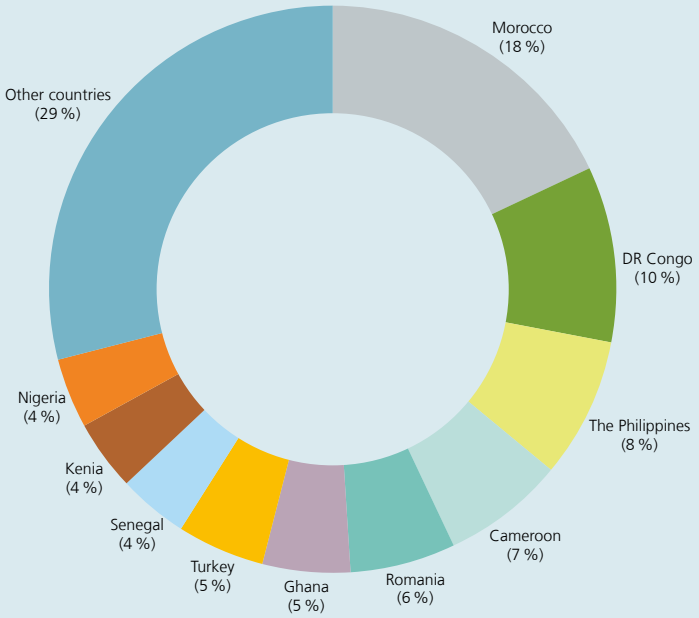


Overview of money remittance in Belgium

Money transfers by all money remitters present in Belgium

(2019, yearly total, payment institutions established in Belgium or other EEA Member States)

Chart – Top-10 Country Corridors in number of transactions IN & OUT money transfer flows



At the end of 2019, the total amount of incoming and outgoing money transfers via money remitters was € 1 546.8 million, an increase of 17.19 % and represented 5.798 million transactions, or an average amount of € 267 per transaction. Belgian payment institutions accounted for € 583.9 million, or 37.75 % against € 962.8 million of all EU money remitters active in Belgium and took a share of 42.89 % in the total of processed number of transactions in Belgium. The increase is due to the establishment of new institutions, mainly relocations of UK institutions in Belgium as a result of Brexit.

One current trend is the digitalisation of the money remittance business: nowadays, several remitters accept only digital pay inflows and try to pay out as much as possible cashless. As a result, the share of online remittance in Belgium, increased to 28.1 % in terms of value.

Taking into account both incoming (IN) and outgoing (OUT) money transfer flows, Morocco (18 %), the Democratic Republic of Congo (9 %), Turkey (8 %) and Romania (8 %) remain, like last year, the most important countries for the money remittance business taking place in Belgium in terms of value. The newly established money remitters in Belgium have had no significant influence on the importance of the different corridors for the time being although we observed increasing numbers of transactions with Cameroon and the Philippines compared to last year.

BOX 9

Brexit: impact on payment institutions

As was the case for CSDs and CCPs (see box 4), Brexit led to an end of passporting rights for UK payment and e-money institutions in Belgium on 1 January 2021. Belgian payment and e-money institutions that had passported into the UK prior to this date and registered for the temporary permissions regime for passporting EEA firms and investment funds (TPR) set up by the FCA are still able to keep their passporting rights on a temporary basis during a large part of 2021, provided they apply for authorisation in the United Kingdom.

The Bank granted licences to two further payment institutions with a Brexit background last year, namely Sendwave on 24 March 2020 and Jubilee Services on 25 February 2020. Since 2017, seven UK payment/electronic money institutions have been relocated to Belgium. Others may follow suit in the course of 2021.

3.3 Processors of payment transactions

Changes in regulatory framework

There were no changes in the Belgian regulatory framework during the period running from January to December 2020.

Prudential & oversight approach

In 2020, one legal entity which is providing processing services in the Belgian payments market was designated as a systemically important payment processor. In line with Article 6 of the Law of 24 March 2017 on the oversight of payment transactions processors, the NBB's Board of Directors has designated equensWorldline SE as a systemically important processor of payment transactions performed through the Maestro card payment scheme (CPS) based on the data collected for the year 2019.

Table 3

List of systemically relevant payment processors

(as at 31 December 2020)

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.

Processors that qualify as being systemically important have to meet a specific set of requirements that aim to maintain the stability and continuity of retail payments in Belgium. One example of these requirements relates to the obligation for having a comprehensive risk management in the fields of detection, appraisal and development of mitigation measures. The legal framework on payment transaction processors also consists of a strict process for incident reporting to the Bank and the ability for the latter to apply a sanctions regime. Table 3 lists the processors of systemic importance and the schemes for which this status was notified.

Supervisory priorities in 2021

Regarding systemically important payment processors, the main focal point of the Bank will remain cyber resilience. (For Mastercard, see also the next section on card payment schemes.)

3.4 Card payment schemes

Regulatory framework

The regulatory framework devoted to card payment schemes (CPSs) remained unchanged in 2020.

In 2019 and 2020 the Eurosystem developed a new oversight framework for electronic payment instruments, schemes, and arrangements (PISA), a consolidation of existing frameworks in one over-arching set. This PISA framework based on the PFMI is intended to become the reference for Eurosystem oversight of payment instruments, schemes, and arrangements, thereby replacing the existing standards such as the "Harmonised oversight approach and oversight standards for payment instruments" (ECB, February 2009)[1] , the "Electronic money system security objectives" (ECB, May 2003), the "Oversight framework for card payment schemes – Standards" (ECB, January 2008)[2], the "Oversight framework for direct debit schemes" (ECB, October 2010)[3] and the "Oversight framework for credit transfer schemes" (ECB, October 2010)[4].

The PISA oversight framework aims at addressing recent regulatory changes (e.g. PSD2 and linked RTS and guidelines) and payment linked to technological developments. It can be considered as complementary to the existing oversight of payment systems and the prudential supervision of payment service providers. It includes an assessment methodology and an exemption policy. Schemes and arrangements of a certain importance and level of risk will be classified based on specific criteria relating to the size of the end user population, market penetration and geographic relevance and will have to comply with the requirements of the framework. The framework, assessment methodology and exemption policy have been submitted to a public consultation in November and December 2020[5] and are expected to be adopted in the course of 2021.

Oversight approach

In the euro area, the sound and safe functioning of card payment schemes is monitored by central bank oversight. The ECB, in cooperation with the Eurosystem national central banks, is in charge of the standard-setting process

1 Harmonised oversight approach and oversight standards for payment instruments (ECB, February 2009): https://www.ecb.europa.eu/pub/pdf/other/harmonisedoversightpaymentinstruments2009en.pdf.
2 Oversight framework for card payment schemes – Standards (ECB, January 2008): https://www.ecb.europa.eu/pub/pdf/other/oversightfwcardpaymentsss200801en.pdf.
3 Oversight framework for direct debit schemes (ECB, October 2010): https://www.ecb.europa.eu/pub/pdf/other/oversightframeworkdirectdebitschemes2010en.pdf.
4 Oversight framework for credit transfer schemes (ECB, October 2010): https://www.ecb.europa.eu/pub/pdf/other/oversightframeworkcredittransferschemes2010en.pdf.
5 Public consultation on the draft Eurosystem oversight framework for electronic payment instruments, schemes and arrangements (europa.eu). Available at https://www.ecb.europa.eu/paym/intro/cons/html/pisa_oversight_framework.en.html.

regarding the oversight framework, as well as the planning of assessments to be undertaken in all jurisdictions. For domestic CPSs, the compliance assessment is, as a rule, conducted by the NCB of the country where the governance authority of the CPS is established. The resulting assessment report is then peer reviewed by representatives of other Eurosystem NCBs before being submitted to the ECB and the Governing Council for publication. The monitoring of ongoing compliance also falls within the competence of the NCB from the jurisdiction where the CPS is legally established. NCBs have the discretion to apply any additional measures they deem relevant for the CPS under their oversight. The Belgian domestic CPS, Bancontact, is subject to oversight by the Bank. Therefore, the results of any assessment of its compliance with the Eurosystem CPS standards are peer reviewed at the Eurosystem level.

For international CPSs, the process is similar except that (i) the assessment work is shared among the members of the assessment group made up of representatives of the NCBs having a legitimate interest in overseeing the international CPS, the coordination of which is ensured by the lead overseer, and (ii) the peer review is de facto undertaken by the other members of the assessment group. This is the case for Mastercard Europe (MCE), established in Belgium, and for which the Bank ensures the role of overseer within the Eurosystem framework coordinating the assessment group.

Regarding MCE which qualifies both as a CPS and as a SIPS, the new PISA framework explicitly stipulates that it will take into consideration the results of every oversight duty performed under the monitoring of its continuous compliance, as a SIPS (see section 3.1), with the requirements of the SIPS Regulation.

In addition to the above-mentioned frameworks, the Regulation on interchange fees for card-based payment transactions (IFR) requirement on the unbundling of scheme and processing activities within the same legal entity also applies to MCE and Visa Europe. The designated national competent authorities of eight Member States in charge of enforcing the unbundling requirement for MCE and Visa Europe have agreed that the Bank (for MCE) and the UK Payment Systems Regulator (PSR, having supervisory competence for Visa Europe established in London) to set up the cooperative mechanism for monitoring compliance with IFR Article 7.1.a. The Bank was formally designated by seven other NCAs as lead NCA in charge of the coordination of the working group devoted to MCE. In its capacity as NCA for MCE, the Bank has been duly informed by MCE about the effective measures put in place to comply with this Regulation.

Based on a detailed questionnaire commonly agreed upon in the cooperative working group, the Bank has (a) collected from MCE its answers in substance and underlying evidence, (b) completed its provisional analysis of its compliance with the so-called IFR and related RTS, and (c) shared its analysis with the cooperative working group members.

Oversight priorities in 2021

It remains to be established whether the assessment of MCE under the perspective of the Cyber Resilience Oversight Expectations for FMIs (CROE[1], which define the Eurosystem's expectations in terms of cyber resilience) is going to be triggered by mid-2021 or at another juncture. The CROE analysis would apply in practice to MCE with no distinction being made between its both qualifications as a SIPS and as a CPS. This decision will depend on the progress achieved in the assessment of MCE as a SIPS (which is a long-lasting duty *per se*).

Stemming from the designation of MCE as a SIPS, particular focus is put on assessing its compliance with the SIPS Regulation (encompassing the PFMI requirements) and the CROE requirements. These assessments will be

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 enables 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.

performed via a joint assessment group (JOT) under the coordination of the NBB and the ECB, consisting of participating Eurosystem NCBs.

After receipt and integration of the contributions from the members of the cooperative working group, and potential subsequent contributions from MCE, a final report, entitled "analysis of the compliance of MCE with IFR Article 7.1.a)" will be drafted by the end of the third quarter of 2021. As a reminder, this part of the IFR for which the Bank acts as lead NCA does concern the monitoring of the effective separation between scheme and processing activities under the perspective of the accounting, organisation and decision-making processes.

Regarding the IFR cooperation mechanism for ensuring compliance of MCE with IFR Article 7.1.a, the assessment exercise, performed by the whole cooperative working group, is expected to be finalised by the third quarter of 2021.

The next step regarding oversight of Bancontact as a CPS will be an assessment based on the new PISA framework. It should be conducted in the context of a Eurosystem-wide exercise to be decided after the finalisation of the PISA Framework.