3. Payments

The Bank has a broad responsibility in the area of payments and adopts the role of both overseer and prudential supervisor, as illustrated in chart 4 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 the 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.

The Bank also participates in the cooperative oversight framework of CLS, a payment-versus-payment (PVP) settlement system for foreign exchange (FX) transactions. The U.S. 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.

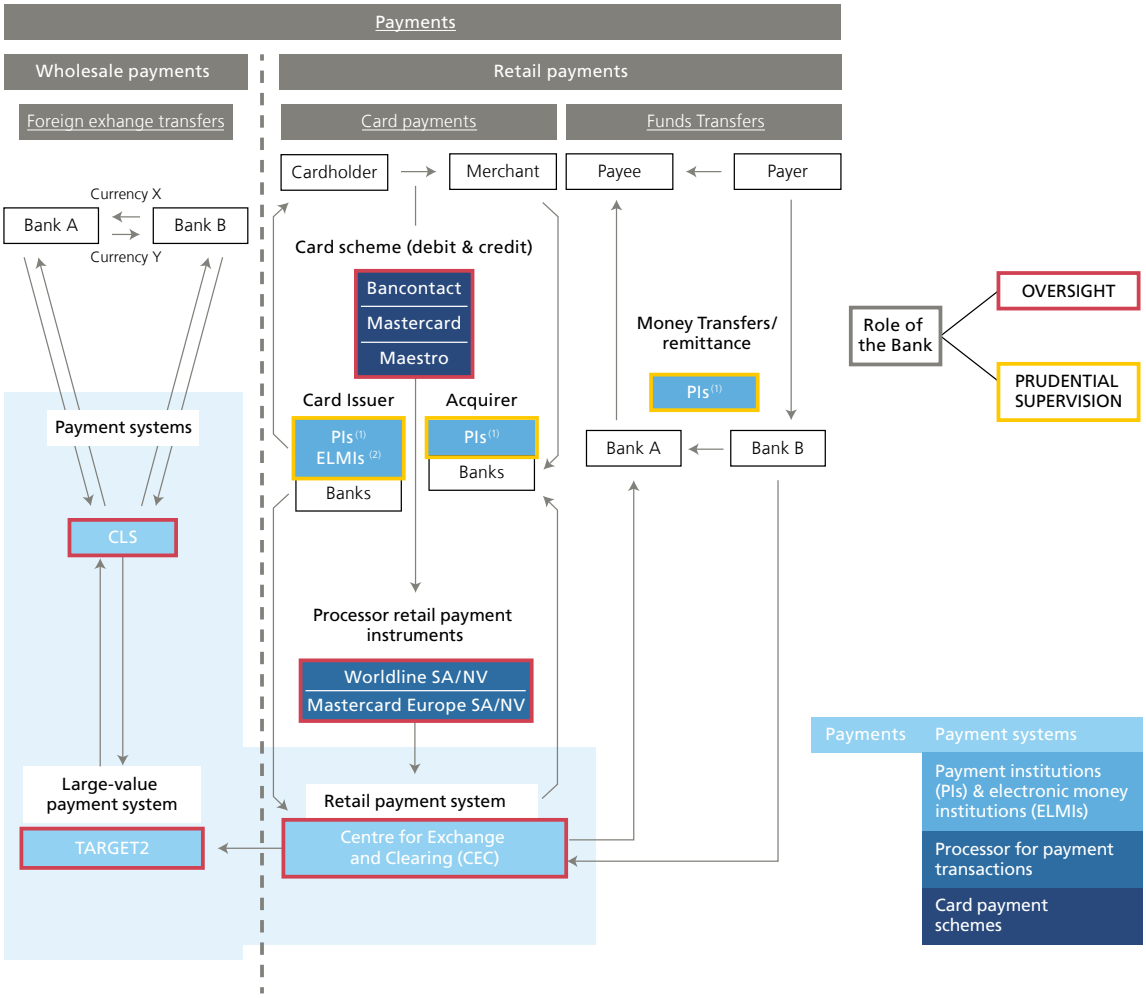
As acquirer[3] and processor of retail payment instruments in Belgium, Worldline SA/NV is subject to both prudential supervision and oversight. The Bank's activities in that respect are covered in section 3.3.

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 governance body).

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

Chart 4

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



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

BOX 8

Impact of COVID-19 on the payments sector

Given the widespread nature and ubiquity of payments in economic life, both the Belgian and international payments market has been significantly and profoundly affected by COVID-19. Even though existing payment infrastructures and payment service providers were able to maintain their operational continuity, the pandemic, together with the subsequent government measures, did generate a substantial and asymmetric shock on the processed number and value of processed transactions for the industry. Moreover, due to the diverse means of payment available for end users, ranging from both cash to credit transfers, this effect was more pronounced for certain service providers than for others.

Based on additional, *ad-hoc* reporting for the sector since the early phase of the government's measures in Belgium, the Bank has been able to estimate a general decline of over 30 % in the value of processed card payments within Belgium at the point of sale (i.e. in-store payments) during the first month of the lockdown, compared to the same period of the previous year. This observation is in line with the figures recorded in other European countries. Yet, Belgian e-commerce card transactions surged during this period with an increase of over 20 %, both in terms of value and volume. This trend was probably due to a shift in consumer spending habits during the initial phase of the measures announced by the government.

Next to this, cash intensive payment services and travel related payment solutions were significantly hit. For example, both the number and value of transactions for certain cash-based money remittance providers in Belgium declined by more than 50 % in the first week of the lockdown period, compared to the same period the previous year. But cross-border payments based on credit transfers rose significantly for specialised payment institutions over this period.

As these figures illustrate, COVID-19 has left a profound and diverging impact on existing payment flows and payment habits. For example, the limit for making a card payment without strong customer authentication (SCA) was lifted from € 25 to 50 for one-off payments with a cumulative threshold raised from € 50 to 100. This increased the number of contactless payments considerably and will probably further enhance the growth and establish this payment habit. In view of the ongoing nature of the pandemic, the Bank expects the effect of this shock on both individual actors and the broader payments landscape to continue for the foreseeable future.

3.1 Payment systems

Changes in regulatory framework

There were no changes in the Belgian regulatory framework in the course of the period running from April 2019 to April 2020.

Oversight approach

The Bank is responsible for the oversight of the CEC, the Belgian domestic retail payment system. The main change in the system was the launch, on 4 March 2019, of a platform developed and run by the French company STET enabling the processing of instant payments (IP). Although the technical platform supporting IP processing and settlement is technically separated from the existing one and has specific features (e.g. settlement based on pre-deposited amounts held by the system on a technical account in TARGET2), it is integrated into the existing automated clearing house as an additional functionality and not as a new system.

The Bank as overseer has been monitoring the development of the IP platform and its specific features such as the establishment of a technical account in TARGET2. Despite the demanding nature of the system, which requires availability in real time not only of the central platform but also the sending and receiving banks, as well as their quick interaction (the payment must be finalised in less than 5 seconds) for the execution of a payment, the IP functionality started smoothly with no significant incidents. The volumes processed are increasing steadily. In 2019, 60 million IP operations were processed with peaks at more than 400 000 operations per day. By the end of 2019, IP represented about 12 % of all credit transfers processed by the system and, on the whole year, about 0.4 % of the total volume. Interoperability with other IP systems should be the next step for the CEC IP. The systems to be connected are the French IP system[1] as well as the pan-European systems TIPS and RT1. From a technical perspective, the necessary features are already in place at system level.

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. During the 2019 classification exercise of payment systems, the Eurosystem concluded that MCE ought to be listed as another systemically important payment system with the ECB and the Bank, as joint lead overseers (see section 3.4).

The CLS Oversight Committee has monitored, among others, CLS' projects to further reduce risks in the FX markets. CLSClearedFX is a service that allows CCPs and their clearing members to safely and effectively mitigate settlement risk when settling cleared FX products. CLSNet is a bilateral payment netting calculation solution, operating on a distributed ledger technology (DLT) platform. CLSNow enables intraday PVP settlement (provided that the payment systems of both currencies are open) – currently transactions are settled gross on a bilateral basis and for a limited number of currencies.

Supervisory priorities in 2020

In 2020, the Bank will continue to pay specific attention to the development of the CEC's cyber resilience. The Cyber Resilience Oversight Expectations for FMIs (CROE)[2] will be used as standard to assess the CEC's maturity in this field. Future developments in the CEC platform (IP and legacy) will also be covered in the oversight framework.

1 The same IP technical platform is used by the French market, but the Belgian and French markets are separate user groups, and it is not yet possible to carry out IP between them.

2 Link available here: https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf.

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.

In 2019, the last Royal Decree[3] 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[4] (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[5], which is applicable to all institutions under supervision of the Bank, including 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.

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 (publication in the Belgian Official Gazette of 26 March 2018).

3 Royal Decree of 21 March 2019 approving the rules of the National Bank of Belgium on own fund requirements of electronic money institutions.

4 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.

5 Circular 2019_19 on the guidelines of the European Banking Authority of 25 February 2019 on outsourcing.

BOX 9

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 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

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. 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 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 still based on the use of the card details (as printed on the payment card), sometimes combined with an SMS one-time password (OTP) or a biometric authentication solution on a mobile device (e.g. a fingerprint or FaceID). As the above-mentioned Opinion stated unequivocally that printed card credentials do not constitute any factor in strong customer authentication, the issuers of such payment cards (credit institutions, payment and electronic money institutions) needed to find alternative authentication solutions that can ensure a continued two-factor authentication that meets the requirements of strong customer authentication under the RTS on SCA & CSC.

The second concern related to the 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, and thus for cases where the application of SCA was not considered by law to provide additional value in terms of reducing fraud or ensuring security. Examples of this 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.

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).

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. Before the summer of 2019, it became clear that this would not be achievable by 14 September 2019.

The combination of these two concerns with a strict adherence to the entry into force of the SCA requirements on 14 September 2019 had the potential to negatively impact EU customers who made use of payment cards in online commerce. The changes SCA introduces require online merchants to make changes on their websites (in order to support the exceptions to SCA) as well as customers to change the way they authenticate with their payment card in the online environment. They also require card issuers to issue their customers with SCA-compliant cards. It was considered 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 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 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 available under the condition that PSPs have set up a migration plan, have agreed the plan with their CA, and execute 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.

Over the 2019 summer period, the Bank conducted an analysis of the state of readiness of the Belgian market, concluding that the main issues were related to the second concern listed above and mainly in relation to online commerce via Visa, Mastercard and American Express card schemes. Furthermore, it was considered that Belgian online merchants need to migrate to new protocols allowing for full use of the exceptions to SCA. Only a small number of Belgian issuers face compliance issues in relation to the use of authentication methods for payment cards that are not SCA-compliant (first concern listed above).

Based on this analysis, on 28 August 2019, the Bank leveraged the supervisory flexibility option provided by the EBA setting out its expectations regarding market implementation – in the framework of online commerce – of the SCA procedure through the issuance of a Prudential Announcement aimed at all Belgian issuers of payment cards and Belgian acquirers of card transactions made in the framework of online commerce. The Bank referenced the aforementioned EBA Opinion, reiterated that the legal deadline of 14 September 2019 for the entry into force of SCA remained in place but acknowledged the challenges for the Belgian card payment industry in meeting this deadline and the need to work together with the relevant stakeholders (payment services providers, card schemes, merchants and consumers associations) and to agree on a reasonable and acceptable plan to migrate – as soon as reasonably possible after 14 September 2019 – for the industry to implement SCA for card payments in online commerce.

The Bank worked closely with the Belgian card payment industry to agree as soon as possible on a reasonable migration plan that encompasses a blueprint for compliance and readiness, a timetable for achieving this, and key milestones and targets to deliver improved security of customer authentication and fraud reduction along the way. In the first half of 2020, the roadmap for this migration was further finalised at Belgian level between the involved stakeholders and was published on the Bank's website in early May 2020[1]. The objective of this migration plan is twofold: i) defining a realistic and feasible migration plan within the applicable deadline and ii) setting milestones to ensure a seamless and secure payment experience for merchants and consumers after the migration period.

The Bank clarified to the market that it expects all stakeholders covered by the migration plan, and in particular relevant PSPs, to fully comply with it and meet the agreed milestones and targets in order to be compliant with the SCA requirements by the final delivery date to be set out in the plan. In order to benefit from this plan, PSPs will have to provide the Bank with sufficient evidence that they have taken appropriate steps to comply with the SCA requirements at the final delivery date set out in the plan.

The Bank deliberately chose not to issue an end date for this migration as it was of the opinion this should be set at pan-European level. Accordingly, on 16 October 2019, the EBA published an Opinion on the deadline for the migration to SCA for e-commerce card-based payment transactions, effectively aimed at harmonising the deadline for supervisory flexibility by CAs in order to avoid divergent end dates for compliance with the SCA requirements. Given the intensively cross-border nature of online commerce in Europe, especially in Belgium, as well as the cross-border nature of acquiring services, it is of vital importance to ensure a common end date for supervisory flexibility. The EBA established this end date at 31 December 2020 and the Bank adheres to it.

Following publication of the Prudential Announcement, the Bank has both attended and hosted Belgian card payment industry meetings in order to help guide the birth of a reasonable and acceptable migration plan with concrete and verifiable milestones for all relevant PSPs towards full compliance with the requirements of SCA.

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. 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.

(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.

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

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. However, provided the dedicated interface meets four requirements listed in the RTS on SCA & CSC, an ASPSP can be exempted by its CA from the requirement to foresee a contingency mechanism.

On 4 December 2018, the EBA further specified these four requirements into nine guidelines through its "Guidelines on the conditions to benefit from an exemption from the contingency mechanism under Article 33(6) of Regulation (EU) 2018/389 (RTS on SCA & CSC)". The Bank transposed these Guidelines on 19 March 2019 into its supervisory practice through issuing its Circular Letter 2019_04, at the same time detailing the application process for Belgian ASPSPs to obtain such an exemption from the Bank.

During the summer of 2019, the Bank received 18 applications for exemption from the contingency mechanism from Belgian credit institutions, one from a Belgian payment institution and one from a Belgian institution for electronic money. Twelve applications were granted before the entry into force of the RTS on SCA & CSC on 14 September 2019. Several more applications have been accepted since then.

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 will rather incrementally continue as new versions of the dedicated interface are brought into production.

Throughout 2019, the Bank engaged proactively with Belgian ASPSPs in order to clarify the relevant legal framework and its interpretation. Since the entry into force of these requirements, the Bank has been monitoring compliance by ASPSPs and TPPs and will continue facilitating dialogue between them where concerns may arise.

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 aims to support the objectives of PSD2 of enabling customers to use new and innovative payment services offered by TPPs by addressing a number of issues regarding the interfaces provided by ASPSPs to TPPs. It clarifies a number of 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 expects the sector to comply with this Opinion by 31 December 2020 at the latest.

Use of alternative techniques to access payment accounts

In the course of 2019, alternative techniques to access payment and other accounts held with Belgian ASPSPs made their entry into the Belgian market on a wider scale. This points to the rising popularity and adoption of business models seeking value in account information (and aggregation) – even beyond the scope of PSD2 – and payment initiation services.

These alternative techniques can be split into two categories: (i) screen scraping of online banking websites and (ii) reverse engineering of the mobile banking channel. In relation to the scope of PSD2, the RTS on SCA & CSC clearly sets out the communication standards between ASPSPs and TPPs. The Bank has been closely examining the detailed workings of both techniques, with a strong focus on the second one given its rising use in the Belgian market.

The Bank is convinced that a comprehensive answer to the use of alternative techniques both within and beyond the scope of PSD2 should be formulated and has been raising awareness about these issues at EU level accordingly. In this vein, the EBA clarified in its Q&A tool relating to PSD2 that ASPSPs should allow TPPs, as part of the contingency mechanism in Article 33(4) of the Delegated Regulation, to use all interfaces made available by the ASPSP to its payment service users (PSUs) for accessing their payment accounts online directly. This includes not only the ASPSP's internet banking interface, but also the ASPSP's mobile banking application made available by the ASPSP to its PSUs, where applicable. The latter does not however imply that TPPs have an automatic right to access the ASPSP's proprietary mobile banking interface that connects the ASPSP's mobile banking app to the ASPSPs' backend systems. It is the ASPSP's responsibility to ensure that TPPs can be identified and can rely on the authentication procedures provided by the ASPSP to its PSUs, in accordance with the requirements of PSD2 and the Delegated Regulation.

Furthermore, the EBA confirmed that TPPs accessing the PSUs' payment accounts using the contingency mechanism in Article 33(4) of the Delegated Regulation should also comply with their respective obligations under Article 33(5) of the Delegated Regulation, as well as with any other applicable EU legislation. In particular, access by TPPs via the PSU interface(s) should not be used as a way of circumventing the application of strong customer authentication by the ASPSP.

Supervisory Priorities in 2020

The Bank's main supervisory activities in 2020 will primarily consist of i) authorisation of new payment institutions and electronic money institutions and ii) monitoring implementation of the requirements related to the RTS on strong customer authentication and common and secure communication within the Belgian market.

With regard to the first activity, the Bank expects a further uptake of firms, both start-ups and incumbents, wishing to apply for the required authorisation to be able to provide payment initiation and account information services. Within this context, the Bank furthermore observes the following trends with regards to the business models of new service providers:

- specialised payment service providers targeting the payment activities of small and medium-sized enterprises (SMEs);
- specialised payment service providers aiming to automate, optimise and enrich payment data processing; and
- a changing offer of the incumbent banking sector to also provide new services by taking up a role of third-party provider and to access accounts of their competitors.

Regarding the first trend, the Bank has observed that a growing number of non-bank payment service providers, i.e. payment institutions and electronic money institutions, are trying to develop a competitive and personalised payment service for SMEs. New service providers argue that this is mainly driven by the fact that SMEs often require specific, individual payment solutions, which have only to a limited extent been provided by the market up to now.

The second observed trend relates to the increased data centricity in the service offering of non-bank payment service providers. Most observed business models revolve around the aggregation of account balances and the provision of digitally tailored and targeted financial services for SMEs, such as financial planning, budgeting and management. In this context, several actors are also focusing on automation of certain business processes, such as those related to cash flow management and accounting, in which account information is integrated.

In parallel to the emergence of these new market actors, existing incumbents are also focusing on integrating these new services, i.e. account information and payment initiation, into their existing product offering. The expectation for 2020 is therefore that more Belgian banks will launch the possibility to consult payment accounts held with other Belgian banks in their own channels as well as to initiate payment orders from that other payment account.

With regard to the second foreseen activity of the Bank in 2020, that of monitoring of the 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 the full deployment of payment initiation and account information services within the market (for more details, see box 9).

For SCA, the focus will be on ensuring that the migration plan is 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 developments taking place within this context and ensuring the creation of stable and fully functional dedicated interfaces enabling the provision of TPP services in the Belgian market. Furthermore, the Bank will continue its work in relation to the use of alternative techniques for accessing payment and other accounts.

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.

BOX 10

Money remittance in Belgium

In 2019, two online money remittance companies were granted a licence by the Bank. In total, seven money remittance companies were listed as Belgian payment institutions at the end of 2019. Belgian payment institutions have an agent network of 244 agents in Belgium and 7 998 agents[1] in other EEA countries. In addition to the 244 Belgian agents, 1 657 agents from other European payments institutions are active in Belgium.

At the end of 2018, the total amount of incoming and outgoing money transfers via money remitters was € 1 319.9 million. Belgian payment institutions accounted for € 356.9 million, or 27.04 % against € 962.9 million of all EU money remitters active in Belgium.

Taking into account both incoming (IN) and outgoing (OUT) money transfer flows, Morocco (22 %), Turkey (10 %) and Romania (9 %) are still the major countries for the money remittance business taking place in Belgium in value terms (chart, left-hand panel). By number of transactions, Morocco (24 %), the Democratic Republic of Congo (12 %) and Romania (8 %) account for the largest share (chart, right-hand panel).

1 92 % of the agents work in name and behalf of Moneygram International, which re-located from the UK to Belgium at the end of 2018 due to Brexit.

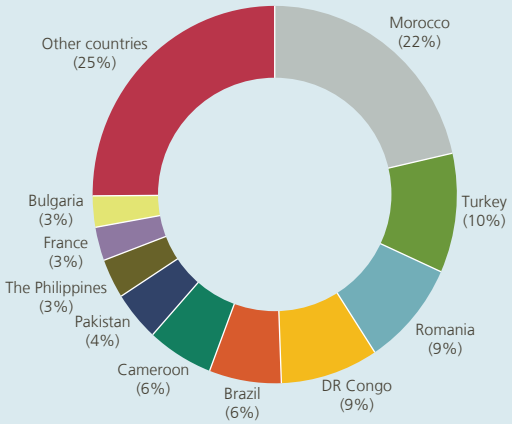
Overview of money remittance in Belgium

Money transfers by all money remitters present in Belgium

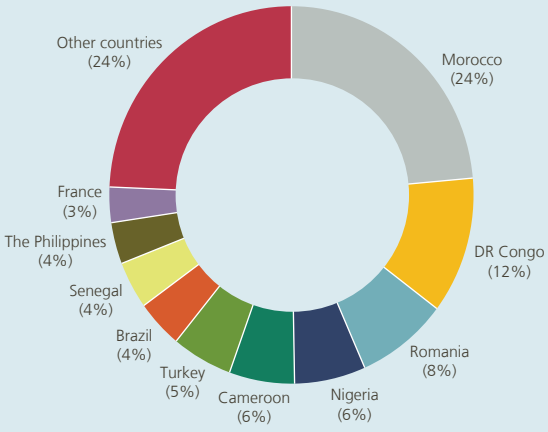
(2018, yearly total, payment institutions established in BE or other EEA Member States, IN & OUT money transfer flows)

Chart – Top-10 Country Corridors

In value



In number



3.3 Processors of payment transactions

Changes in regulatory framework

There were no changes in the Belgian regulatory framework in the course of the period running from April 2019 to April 2020.

Prudential and oversight approach

In 2019, 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 Mastercard Europe as a systemically important processor of payment transactions performed through its card payment scheme (CPS) Maestro based on the data collected for the year 2018 from Mastercard Europe as a CPS.

Processors which qualify as being of systemic importance 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.

Supervisory priorities in 2020

The Bank will keep its focus on cyber resilience of systemically important payment processors and continue to monitor the evolution in that respect. As a part of its monitoring activities, the Bank carried out an on-site "IT security inspection" on Worldline in 2019. Implementation of the action plan designed to answer the recommendations issued by the Bank will be monitored in 2020. (For Mastercard, see the next section on card payment schemes.)

3.4 Card payment schemes

Regulatory framework

The regulatory framework devoted to card payment schemes remained unchanged over the period running from April 2019 to April 2020.

Oversight approach

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

During the 2019 classification exercise of payment systems, the Eurosystem concluded that MCE ought to be listed as a systemically important payment system[1] (SIPS), due to its important payments clearing function. This additional qualification[2] requires MCE to comply with the requirements of the SIPS Regulation (including the CPMI-IOSCO PFMIs referred to above) and the Cyber Resilience Oversight Expectations for FMIs (CROE), which define the Eurosystem's expectations in terms of cyber resilience.

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[3] which of the three maturity levels (Evolving, Advancing, Innovating) must be achieved by the systems according to their risk profiles and specific activities.

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) would set up a cooperative mechanism for monitoring compliance with IFR Art. 7.1.a. The Bank was formally designated by seven other NCAs as lead NCA in charge of coordinating the cooperative 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, and (b) started to assess compliance with those implemented measures.

Oversight priorities in 2020

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 performed in coordination with an assessment group, consisting of participating Eurosystem NCBs, and under the joint lead oversight of the Bank and the ECB.

Regarding the IFR cooperation mechanism for ensuring compliance of MCE with IFR Art. 7.1 a, the assessment exercise, performed by the whole cooperative working group, is expected to be finalised at the 2020 Q4 / 2021 Q1 horizon.

The compliance of Bancontact with article 7.1 of the IFR will be reviewed in the course of 2020. Bancontact is fully compliant with the current oversight standards. This assessment will be reviewed in case of significant evolution of the scheme or if the applicable Eurosystem oversight framework is updated.

1 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020XB0026&from=EN.
2 Mastercard remains a CPS, the additional qualification as SIPS only covers clearing and settlement function of the CPS.
3 The eight domains covered by the CROE are Governance, Identification, Protection, Detection, Response and Recovery, Testing, Situational awareness and Learning and evolving.