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 4 below. Oversight focuses on payment systems, instruments[1] and schemes[2] while prudential supervision targets payment service providers (PSPs). These approaches are complementary: while oversight concentrates on the sound and safe functioning of payment systems, payment instruments, payment schemes or other payment infrastructures, supervision pursues safe, stable and secure financial institutions 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 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. CEC is the domestic retail payment system (RPS) processing intra-Belgian domestic payments.

The Bank also participates in the cooperative oversight framework of CLS Bank, a US-based payment-versus-payment (PvP) settlement system for foreign exchange (FX) transactions. CLS has been designated as a systemically important financial market utility by the US Financial Stability Oversight Council with the US Federal Reserve Board as the Supervisory Agency. The Federal Reserve Bank of New York supervises CLS under delegated authority from the Federal Reserve Board. 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 Bank), with the US Federal Reserve acting as lead overseer and performing the secretariat function for the OC.

Prudential supervision of Payment Institutions (PIs) and Electronic Money Institutions (ELMIs) – a relatively new sector of PSPs which may offer since 2009, just like banks, payment services in Europe – is described in section 3.2. 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.

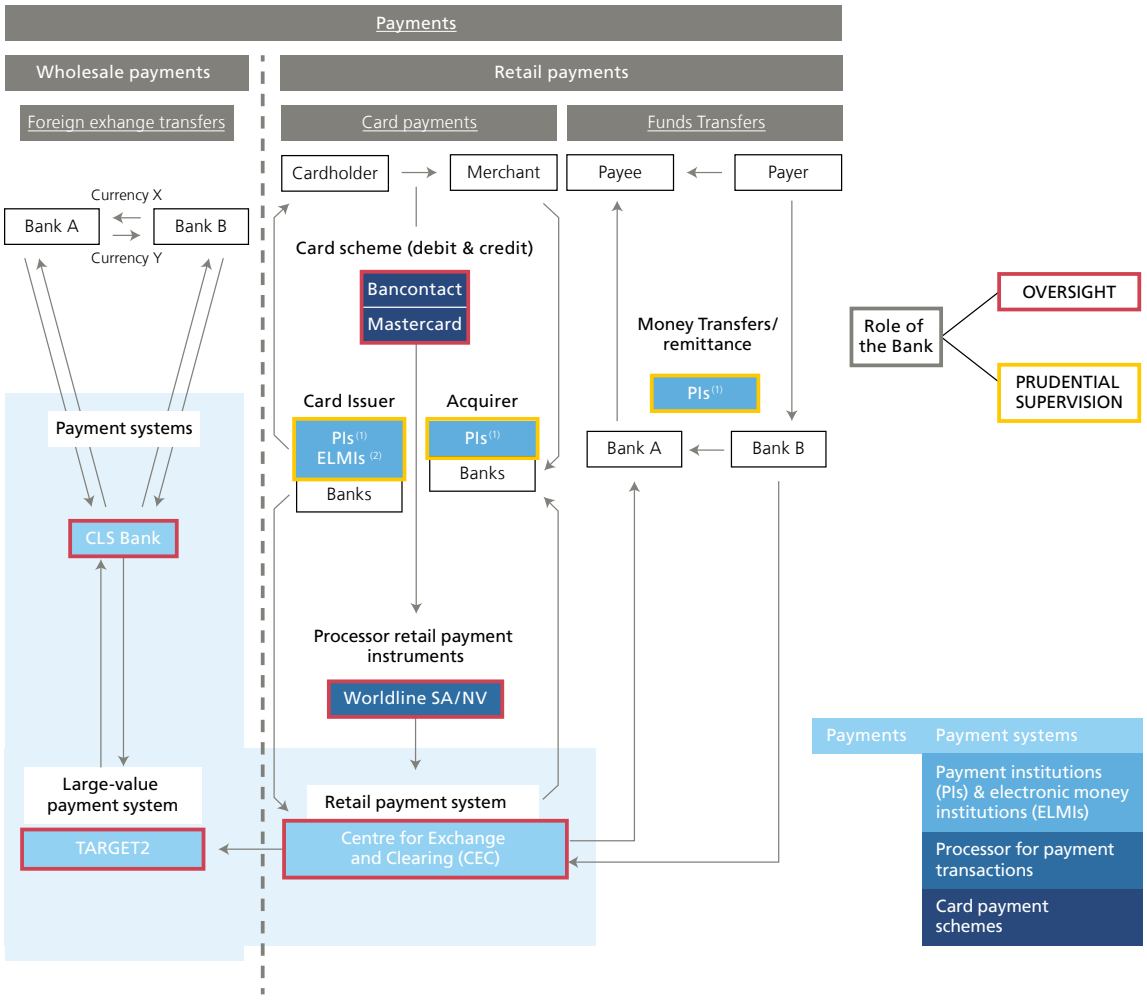
As acquirer[3] and processor of payment transactions in Belgium, Worldline SA/NV is subject to both prudential supervision and oversight. The Bank's activities in that respect are covered in section 3.3.

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 Acquiring of card payments is the 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.

Section 3.4 covers the two payment card schemes overseen by the Bank : the domestic Bancontact scheme and the international Mastercard scheme.

Chart 4

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



1 Payment institutions (PIs)
- *Card acquiring and processing : Alpha Card, Alpha Card Merchant Services, Airplus International, Worldline, Lufthansa Airplus ServiceKarten, SIX Payment Services ;*
- *Money Transfers / Remittance : Belmoney Transfert, Gold Commodities Forex, HomeSend, Money International, MoneyTrans Payment Services, Travelex, WorldRemit, Transferwise Europe, Moneygram ;*
- *Direct Debit : EPBF ;*
- *Hybrid : BMCE EuroServices, Cofidis, eDebex, iBanFirst, Oonex, PAY-NXT, Santander CF Benelux, Ebury, Digiteal, Cashfree ;*
- *Account Information Services & Payment Initiation Services : Isabel, Let's Didid, Accountable.*

2 Electronic money institutions (ELMIs)
- *Buy Way Personal Finance, Fimaser, HiPay ME, Imagor, Ingenico Financial Solutions, Ingenico Payment Services, Viva Payment Services, Paynovate.*

Situation as of end of April 2019 covering Belgian PIs and ELMIs, as well as foreign entities with a branch in Belgium.

3.1 Payment systems

Changes in regulatory framework

In December 2018, the ECB published the *Cyber Resilience Oversight Expectations for FMIs*, in short the CROE, defining the Eurosystem's expectations in terms of cyber resilience. They are based on the guidance on cyber resilience[1] for FMIs published by the CPMI-IOSCO in June 2016. The expectations are applicable to both large-value and retail payment systems, and more generally to all FMIs. The CROE aims at providing overseers with a clear framework to assess the cyber resilience of systems under their responsibility and to 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 the eight domains covered[2] which of the three maturity levels proposed (Evolving, Advancing, Innovating) must be achieved by the systems, according to their risk profiles and specific activities.

Oversight approach

The Bank is responsible for the oversight of the CEC, the Belgian domestic retail payment system. In 2018, the focus of the CEC was put on the development of the Instant Payments (IP) platform (see Box 9) that was launched on 4 March 2019. Unlike in other countries, the Belgian IP platform will not be considered as a distinct payment system but will be integrated in the existing automated clearing house as an additional functionality. The technical platform supporting processing and settlement of IP was developed by the French company STET, which, since 2013, is also operating the CEC's processing platform for all payment instruments used in Belgium. The Bank as overseer has monitored *inter alia* the development of the IP platform and its specific features such as the creation of a technical account in TARGET2 as well as the adapted definition of finality, taking into account the real-time nature of IP[3]. The same IP technical platform is used by the French market. However, in a first stage, the two markets will be separate user groups, and it will not be possible to carry out IP between them. Interoperability between the two groups as well as with pan-European systems is expected to be implemented later in 2019.

The CEC's cyber resilience remained in the scope of the Bank's oversight activities in 2018. The Bank required the CEC, which uses SWIFT connectivity services between the system participants and the technical platform operated by STET, to pay particular attention to its participants' compliance with the SWIFT Customer Security Programme. The Bank will make use of the CROE for assessing the CEC's cyber resilience.

With the ECB as the lead overseer, the Eurosystem conducts the oversight of three Systematically Important Payments Systems (SIPS): TARGET2, EURO1 and STEP2. The oversight is conducted on a cooperative basis with all the national central banks in the Eurosystem[4].

1 https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf

2 The eight domains covered by the CROE are Governance, Identification, Protection, Detection, Response and Recovery, Testing, Situational awareness and Learning and evolving.

3 Unlike for the other payment instruments processed in the settlement cycles of the CEC, which become final after settlement of the multilateral net balances in TARGET2, finality in IP is reached for each payment individually after validation of the payment at the level of the CEC IP platform.

4 More detailed information on the cooperative oversight activities relating to the Eurosystem should be provided in the Eurosystem Oversight Report 2018 which is expected to be published by the ECB in the second half of 2019, as well as, for TARGET2, in the system's Annual Report.

BOX 9

Instant Payments

One of the trends currently observed in the development of retail payment systems is the emergence in many countries of infrastructures aiming at processing Instant Payments (IP), also called "fast" or "faster" payments[1]. The Euro Retail Payments Board (ERPB) defines instant payments as *"electronic retail payment solutions available 24/7/365 and resulting in the immediate or close-to-immediate interbank clearing of the transaction and crediting of the payee's account with confirmation to the payer (within seconds of payment initiation)"*. The emergence of IP is one of the consequences of the evolution of societies towards digitisation. On the one hand, new technologies enable the creation of such a real-time payment instrument which provides a suitable alternative to paper-based instruments such as cheques and cash and, on the other hand, the higher level of on-line interaction between people creates the need for such instruments. The usual credit transfers which need one working day (or even more) to be settled on the account of the beneficiary do not meet the new needs arising from this digitised society.

IP mechanisms are being set up around the world. In countries like Australia, China, Denmark, Japan, Sweden, the UK and the US, such mechanisms are already operational. Since early 2019, a domestic IP solution has also been up and running in Belgium and France, and one is planned to start soon in the Netherlands. In Europe, cross-border IP systems are also in place: RT1, the IP solution from EBA Clearing, and TIPS (TARGET Instant Payment Settlement), developed by the ECB as an ancillary service to the RTGS system TARGET2, which was launched on 30 November 2018. These solutions enable the processing of IP between payer and payee using bank services from different countries of the SEPA. By allowing other IP platforms to link to them, those cross-border systems will also foster interconnection between IP mechanisms in Europe.

In order to support interoperability of IP solutions developed in Europe by avoiding the creation of different standards, the European Payments Council (EPC) has developed a specific scheme based on the SEPA Credit Transfer (SCT) called SCT Inst. By the end of 2018, more than 2 000 payment services providers (PSPs) from 16 countries among the 34 European countries and territories composing the SEPA had already adopted it. According to the rules of the scheme, IP, which may not exceed € 15 000 by operation, will be executed in a maximum of 10 seconds.

IP is often presented as a solution to replace the old paper-based cheques which are still used in some commercial sectors and, to some extent, as a substitute for cash, especially when the amounts of the transactions exceed the legal limits for cash payments (€ 3 000 in Belgium). However, it cannot be excluded that IP will be used in other areas such as e-commerce, where cards are now the most frequently used instrument. PSPs might also decide to use IP to support mobile payments schemes.

The introduction of IP has an impact on the traditional PSPs which is not limited to the setting up of a new central platform. Using IP also means that they will need to shift from batch processing of retail payments performed on working days only to real-time processing of the operations on a continuous basis, 24 hours a day, every day of the year. Such a change is likely to have a far-reaching impact on

1 See Committee on Payments and Market Infrastructures (CPMI), Fast payments – Enhancing the speed and availability of retail payments, November 2016.

the technical and organisational processes of the PSPs' internal payment systems, ICT infrastructure and connected applications.

IP might also give rise to specific risks. The need for uninterrupted availability introduces a new perspective for operational risk management processes for the platform, whereas real-time processing makes fraud detection and fulfilment of AML obligations more complex for participating PSPs.

Supervisory priorities in 2019

The Bank will pay specific attention to the CEC's new IP functionality and its first few months of operation. Considering the complexity of the IP processing resulting from near immediate settlement, the focus will be set on operational reliability of the platform and monitoring of the activity.

The CROE will be used to assess and, if need be, support improvement in the CEC's maturity as regards cyber resilience. As CORE-FR – the French SIPS – shares the same technical platform as the CEC, this assessment will be carried out together with Banque de France, STET's lead overseer. The ECB has already decided to assess the SIPS against the CROE, but for non-SIPS (such as the CEC), the launch of a European-wide assessment exercise has not been contemplated yet.

3.2 Payment institutions and electronic money institutions

Changes in regulatory framework

In 2018, the second Payment Services Directive (PSD2) was transposed into Belgian legislation through two Laws. The Law of 11 March 2018[1] repeals and replaces the Law of 21 December 2009 and contains the prudential aspects of PSD2 that fall within the competence of the Bank. Consumer protection topics of the PSD2 were transposed in the Law of 30 July 2018 amending Book VII of the Code of Economic Law for which the Federal Public Service Economy is the competent authority. PSD2 encourages innovation and competition by allowing new players to offer new types of payment services on the market: payment initiation services and account information services. PSD2 also aims for simpler, safer and more efficient payment transactions within Europe[2].

To develop a coherent legal framework at Community level, the Commission has also conferred twelve mandates on the EBA for the technical aspects of the prudential part of PSD2, including five regulatory technical standards (RTS) and seven guidelines (GL). Four of these mandates relate to setting up adequate security measures for electronic payments. The RTSs[3] have direct effect and do not need to be implemented under Belgian legislation to be applicable, whereas the GLs have no direct effect and were transposed into Belgian legislation by NBB

1 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).

2 The Law of 30 July 2018 amending Book VII of the Code of Economic Law (publication in the Belgian Official Gazette of 5 September 2018).

3 RTS on home-host cooperation, RTS on the EBA register, RTS on central contact points, RTS on passporting, RTS on strong customer authentication and secure communication.

Circulars[1]. Under the Law of 11 March 2018, Royal Decrees were issued during the course of 2018 laying down the Bank's regulations on the own funds of Payment Institutions (PIs) and Electronic Money Institutions (ELMIs), regarding waivers from certain legal requirements for limited[2] PIs/ELMIs, and on the registration of limited PIs/ELMIs[3]. One of the priorities was the transitional measures described in the new Law of 11 March 2018. All regulated institutions under PSD1 were required to submit a grandfathering file to continue their activities under PSD2. More specifically, these institutions were required to submit their file to the Bank to demonstrate that they comply with the new requirements under the new Law. The additional licensing requirements tested during this grandfathering process were:

1. The protection of sensitive payment data;
2. Compliance with the EBA RTS on strong customer authentication and common and secure communication standards (RTS SCA/CSC);
3. Having an adequate IT security policy;
4. The reporting to the Bank of operational and security incidents;
5. The collecting of statistics on transactions, fraud and performance;
6. Having the necessary business continuity arrangements;
7. Compliance with rules governing the issuance of card-based payment instruments;
8. Compliance with the rules concerning the management of payment accounts.

As the new Law encourages innovation and competition, new players can enter the payments market and thus new security risks must be considered. Therefore, all institutions must comply with the new rules with a focus on the security of payments. Institutions that cannot demonstrate compliance with the new requirements that are applicable to them have to cease their activities. Another obligation under PSD2's implementation in Belgium is that money remitters have to comply with the requirements for a full licence, and so they can no longer make use of the light regime. See Box 10 on money remittance in Belgium.

The new legislation enables a new category of PIs to gain access to the payments market by obliging the account servicing payment service providers (ASPSPs, mainly banks) to open up the payment accounts infrastructure (so called *open banking*). The accounts are open to new payment services, namely payment initiation and account information. As these new services can involve additional security risks, strict security rules must be complied with by the PSPs (banks, PIs and ELMIs). These new players do not actually handle payment service user funds, and so neither the safeguarding principles for funds of payment service users, nor the capital requirements are applicable. However, the new category of PSPs must endorse a professional indemnity insurance or a comparable guarantee in order to cover their liabilities[4].

The changes in the legal landscape have also been translated into a new application guide published on the Bank's website[5]. It serves as a guideline for obtaining registration as a PI offering account information services only, for registration as a limited PI/ELMI or for a licence as a PI/ELMI. One of the new requirements of PSD2 is to identify and check people with qualified holdings in the PI/ELMI, both at the start of the institution's business and when there are changes in shareholdership of licensed institutions.

1 Circular on fraud reporting, Circular on the criteria on how to stipulate the minimum monetary amount of the professional indemnity insurance, Circular on security measures for operational and security risks, Circular on major incidents reporting, Circular on authorisation and registration. Circular on the conditions to be met to benefit from an exemption from contingency measures under Article 33(6) of Regulation 2018/389 (RTS on SCA).

2 The limited status is designed to allow access to the market to newcomers and innovators with an initial limited scale. Conditions for adopting a light regime include *inter alia* thresholds of activity. For PIs, the monthly average of the total value of payment transactions to be executed in twelve months should not exceed € 1 000 000. For ELMIs, the average amount of outstanding electronic money should not exceed 1.500.000 EUR. PIs should also provide only a subset of payment services listed in PSD2.

3 Royal Decree of 27 April on own fund requirements of payment institutions (http://www.ejustice.just.fgov.be/cgi/article_body.pl?language=nl&caller=summary&pub_date=18-05-8&numac=2018012004), Royal Decree of 3 June 2018 on limited payment institutions and limited institutions of electronic money (http://www.ejustice.just.fgov.be/eli/besluit/2018/06/03/2018012697/staatsblad) , Royal Decree of 30 July 2018 on the registration of limited payment institutions and limited institutions of electronic money (http://www.ejustice.just.fgov.be/eli/besluit/2018/07/30/2018013236/staatsblad), Royal Decree on own fund requirements of electronic money institutions of 21 March 2019 (http://www.ejustice.just.fgov.be/eli/besluit/2019/03/21/2019011377/staatsblad).

4 Articles 73, 89, 90 & 92 of PSD2.

5 https://www.nbb.be/doc/cp/eng/2018/application_guide_payment_institutions.

Prudential approach

The Bank is the national competent authority within Belgium for prudential supervision of PIs and ELMIs. In order to carry out this role, the Bank relies on a wide range of tools, provided by Belgian law, to ensure the secure functioning and solvency of these institutions.

The Bank applies a waiver regime for institutions operating on a limited scale. The goal of the waiver, which is characterised by less strict authorisation and reporting requirements than for a *full* licence, is to allow start-ups and small institutions to enter the market relatively quickly to launch their product or service, while fostering both innovation and competition. The regime, which is optional for EEA Member States, requires them to apply for full authorisation once they reach a certain threshold. If institutions do not reach the threshold, and benefit from the waiver, they are not allowed to passport their services to another EEA Member State. In line with the objectives of PSD2, the waiver regime has been transposed into the Belgian Law of 11 March 2018[1] and its Royal Decrees[2], reducing the previously applicable thresholds for PIs and ELMIs[3] .

A specific application procedure has been established by the Bank for institutions that seek to relocate their business to Belgium. The scope of this particular procedure is strictly limited to PIs and ELMIs that have already obtained a licence in another EEA Member State and which effectively envisage to move their payment services or e-money operations to Belgium. It is worth noting in this context that business decisions for the Belgian market – and by extension the EEA market if they are passported from Belgium – must be taken by the Belgian entity (central administration[4]). Applicants can use their original foreign application file to start from, but this document must be adjusted to the perspective of the Belgian entity and must take into account the Belgian legislation (for example anti-money-laundering rules). In 2018, the Bank received several licence applications from Brexiteers wanting to relocate to Belgium, in order to be able to continue to passport their activities in the EEA after Brexit. As of May 2019, four institutions active as PI in the UK had received a licence as PI in Belgium[5].

For the grandfathering procedure to continue activities under PSD2, the Bank has reauthorised most institutions in the course of 2018, but some of them[6] have ceased their activities as the new PSD2 requirements were too demanding due to their very small business scale. Some of the licensed PIs have applied for (and obtained) an extension of their current activities to offer payment initiation and account information services. No new PIs or ELMIs were licensed in 2018 (except for exempted PIs which had to obtain a full licence in order to continue their activities as money remitter), presumably because of the transition to the new regulatory framework and the preparation for launching new business models. From Q3 2018 onwards however, the Bank was approached by several new (FinTech) players and incumbents with plans to deploy new types of payment activities based on the newly regulated initiation and account information services to test their new business models on viability and regulatory requirements. In February 2019, there were three institutions[7] that received a license or a registration for the new aforementioned activities, which brings the total amount of institutions that may offer these activities to seven[8].

1 Law of 11 March 2018 transposing the PSD2, Belgian Official Gazette 26 March 2018.

2 Royal Decree of 3 June 2018 on limited payment institutions and limited institutions of electronic money, Royal Decree of 30 July 2018 on the registrationof limited payment institutions and limited electronic money institutions.

3 The threshold for PIs is reduced to € 1 000 000 and the threshold for ELMIs to € 1 500 000.

4 See Article 23 of the Law of 11 March 2018.

5 Ebury, Moneygram, Transferwise Europe and WorldRemit.

6 Africash, Instele, and Rent A Terminal Belgium.

7 Isabel and Let's Didid: account information and payment initiation, and Accountable: only account information

8 Accountable, Buy Way Personal Finance, Digiteal, iBanfirst, Isabel, Let's Didid, Worldline.

BOX 10

Money remittance in Belgium

Money remittance is defined in the Payment Services Directive (PSD2) as "a payment service 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".

Money remittance is linked to emigration waves where migrants transfer money to their home country. It is a long-established, basic payment service usually based on cash provided by a payer to a payment service provider (PSP), which remits the corresponding amount to the payee anywhere in the world, for example via a communication network. Nowadays, remitting to another PSP acting on behalf of the payee is increasing.

Since the transposition of the first Payment Services Directive (PSD1) into Belgian legislation in 2009, the money remittance payment service was brought under a prudential supervision regime for the first time. Institutions offering money remittance services for many years had to apply for a licence as payment institution in one of the EEA Member States.

Before being able to start offering money transfers in EEA Member States, the status of payment institution must be requested from the national competent authority (NCA). Despite the presence of a network of banks, there is still a market demand for cash money transfers. At the end of 2018, there were five Belgian payment institutions and 14 established payment institutions from other European countries offering core money remittance services in Belgium.

The estimated total amount of incoming and outgoing money transfers via money remitters in Belgium is about € 1.3 billion on a yearly basis[1]. In 2017, Belgian payment institutions accounted for 14 % of the total amount of incoming and outgoing money transfers of all EU money remitters in Belgium (the chart 1, left-hand panel). About 86 % of the value relates to outgoing money transfers (right-hand panel).

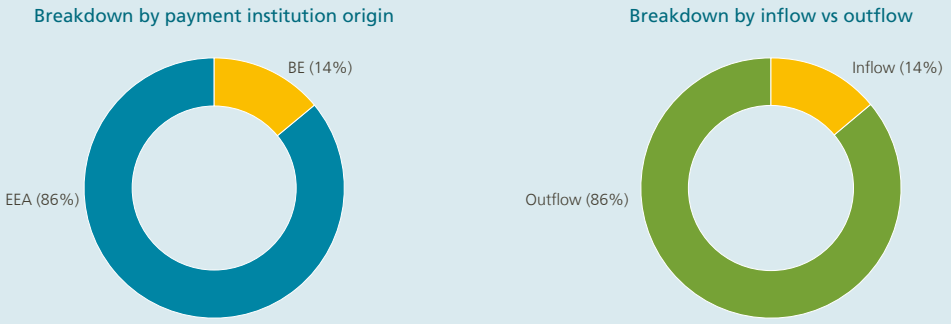
Taking into account both incoming and outgoing money transfer flows, Morocco (21 %), Romania (10 %) and Turkey (9 %) remain the most important countries for the money remittance business taking place in Belgium in value terms (chart 2, left-hand panel). By number of transactions, Morocco (39 %), the Democratic Republic Congo (10 %) and Romania (8 %) account for the largest share (right-hand panel). Chart 3 shows these money transfer in- and outflows per country, in value (left-hand panel) and in numbers (right-hand panel). The data also show inflows from Belgium which relates to payments from one payment institution in Belgium to another whereby the latter has a network for processing payments via corridors on behalf of the former.

1 In 2016, the total amount of incoming and outgoing money transfers via money remitters was € 1 276.2 million. Belgian payment institutions accounted for € 191.6 million against € 1 084.6 million of all EU money remitters active in Belgium. Due to changes in the reporting requirements, more recent data sets are not available at this stage.

Overview of money remittance in Belgium

Chart 1 – Money transfers by payment institutions present in Belgium

(2017, based on value of incoming and outgoing money transfers, yearly total)



Money transfers by all money remitters present in Belgium

(2017, yearly total, payment institutions established in BE or other EEA Member States, IN & OUT money transfer flows)

Chart 2 – Top-10 Country Corridors

(2017, based on value of incoming and outgoing money transfers, yearly total)

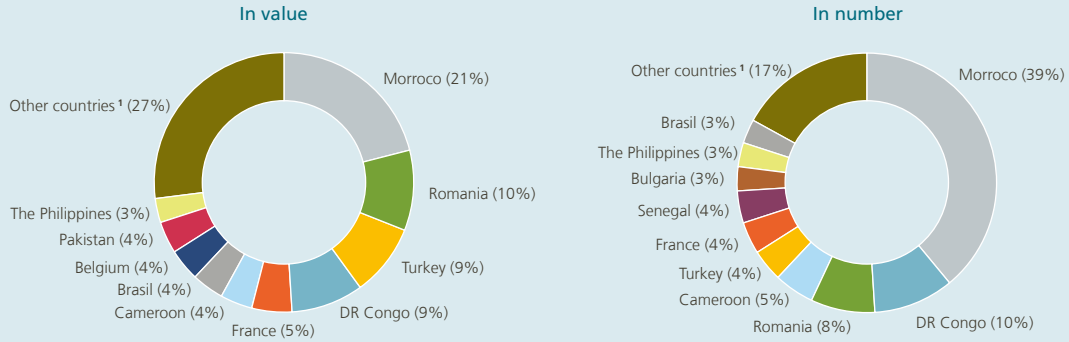
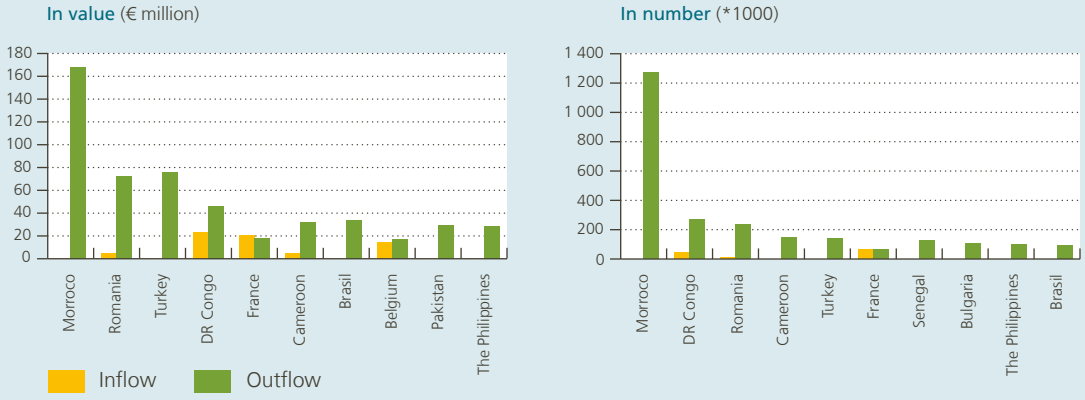


Chart 3 – Money Transfer In- and Outflow per top-10 Country Corridor

(2017, ranking based on value of incoming and outgoing money transfers, yearly total)



Source: NBB.

1 About 45 countries

Supervisory priorities in 2019

The Bank's supervisory activities in 2019 will mainly be driven by the further development of the level 2 (EBA RTSs and GLs) and level 3 (Belgian Circulars) legal framework of PSD2. Since the grandfathering procedure has been implemented and institutions re-licensed under the Law of 11 March 2018, the focus will be on the ongoing supervision and the follow-up on the recommendations that were made in the grandfathering file. For newly authorised institutions, the supervision will focus on the new security requirements. To reinforce security of payment services provided via third-party providers, the use of a specific, dedicated and secured interface will be mandatory from the entry into force as of 14 September 2019 of the RTS on strong customer authentication and common and secure open standards of communication. The dedicated interface will be provided by ASPSPs by so-called APIs (Application Programming Interfaces), ensuring communication and transfer of data between the ASPSPs and third-party providers. The Bank will actively monitor the developments taking place within this context and will also examine how the revised regulatory framework will impact existing business models.

In 2019, the PIs and ELMIs have to report statistical data on fraud related to payment transactions initiated and executed. Moreover, all RTSs and GLs, developed by the EBA under the mandate of the Commission, require the Bank to notify and enforce them with the Belgian payment services industry.

As in previous years, the Bank remains actively involved in the international work by the Commission and EBA to ensure a common and harmonised European approach to implementing PSD2 and to reach maximum supervisory convergence.

The Bank continues to build up bilateral dialogue with FinTech companies and start-ups, notably through its single contact point set up in cooperation with FSMA for the benefit of new players in the market.

3.3 Processors of payment transactions

Changes in regulatory framework

The sound functioning of payment systems processing is a primary objective of the Bank's oversight. With the Law of 24 March 2017 on the oversight of payment transactions processors, the Bank's enforcement of oversight standards and requirements regarding card schemes and their processing has evolved into hard-law-based oversight for systemically relevant payment processors[1]. Some requirements of this Law concerning the obligations of those processors as well as of card payments schemes (CPSs) associated with them have been taken up in a Regulation issued by the Bank. These requirements cover the due diligence that CPSs must conduct when using the services of systemically relevant payment processors, identification and management of risks taken by those processors, continuity of their services and practical arrangements for notification in the event of an incident. The Regulation adopted by the Bank in November 2018 had to be incorporated into a Royal Decree in order to enter into force. This Royal Decree was published on 19 February 2019[2].

Prudential & oversight approach

Worldline SA/NV is the Belgian subsidiary of the French company Worldline which is the payments and transactional services division of the IT services group Atos (see group structure in Annex 2).

1 The list of systemically relevant payment processors can be consulted on the NBB website: https://www.nbb.be/en/financial-oversight/oversight/payment-systems-card-schemes-and-processors/oversight-processors.

2 http://www.ejustice.just.fgov.be/eli/arrete/2019/01/25/2019040243/moniteur (FR) or http://www.ejustice.just.fgov.be/eli/besluit/2019/01/25/2019040243/staatsblad (NL)

From an oversight perspective, Worldline SA/NV has systemic relevance resulting from its significant position in the processing of Belgian debit and credit card payments. It has consequently been designated as a systemically relevant payment processor under the Law of 24 March 2017. It came along with its long-standing regulatory status as payment institution, required for its acquiring activities.

In May 2018, the Worldline Group acquired SIX Payment Services (Europe), the payment services division of the Swiss group SIX. The € 2.3 billion transaction was primarily financed by the issuance of new shares. Although the acquisition took place at the level of the Worldline Group, the Bank, in its capacity as prudential supervisor of Worldline SA/NV, had to formally approve it considering the strategic impact on the payment institution. In terms of card payment operation processing, this acquisition is not expected to entail any significant change in Belgium.

Supervisory priorities in 2019

Cyber resilience is key for a company like Worldline, whose card payment transaction processing and acquiring activities are based on the use of data processing centres and extensive communication networks. In view of the systemic importance of Worldline and equensWorldline as a payment processor in Belgium, the Bank will keep its focus on cyber resilience and continue to monitor the improvements made by the company in this area. Although the ECB's Cyber Resilience Oversight Expectations (CROE)[1] were not originally designed for card payment processors, they are sufficiently flexible to be used in this context and will serve as reference for monitoring the progress made by Worldline in terms of cyber resilience.

Also, the compliance of Worldline SA/NV with the new Regulation supplementing the Law of 24 March 2017 on the oversight of payment transactions processors will be assessed by the Bank.

3.4 Card payment schemes

Regulatory framework

Under Article 7.1 (a) of the EU Regulation on interchange fees for card-based payment transactions (IFR)[2], when payment card scheme governance activities[3] and payment transaction processing activities[4] are performed within the same legal entity, these activities should be unbundled by setting up Chinese walls inside that legal entity in order to put the processing business unit on an equal footing with external payment transaction processing firms. The requirements for this unbundling are set out in the RTS published on 18 January 2018[5] based on which the national competent authorities assess the compliance of each legal entity hosting both scheme and processing activities. The RTS aims to maintain independence between these two activities in terms of (i) accounting (separated profit and loss accounts with transparent allocation of income and expenditure, annual review by an independent and certified auditor of the financial information reported to the national competent authorities), (ii) organisation (i.e. via two separate internal business units located in separate workspaces with restricted and controlled access, distinct remuneration policies, no sharing of sensitive information) and (iii) decision-making process (separate management bodies for the scheme and processing business units, separate annual budget plans).

1 See section 3.1 on payment systems.

2 Regulation (EU) 2015/751 of the European Parliament and of the Council of 29 April 2015 on interchange fees for card-based payment transactions, OJ 19 May 2015, L. 123, 1-15.

3 i.e. rules, licensing, business practices.

4 i.e. services for the handling of a payment instruction between the acquirer and the issuer, including authentication of payment transactions, certification of technical rules, routing towards different market infrastructures.

5 Commission Delegated Regulation (EU) 2018/72 of 4 October 2017 supplementing Regulation (EU) 2015/751 of the European Parliament and of the Council on interchange fees for card- based payment transactions with regard to regulatory technical standards establishing the requirements to be complied with by payment card schemes and processing entities to ensure the application of independence requirements in terms of accounting, organisation and decision-making process, OJ 18 January 2018, L. 13/1-7.

Supervisory tasks have been split between the Belgian Federal Public Service Economy, in charge of monitoring the implementation of all IFR articles relating to consumer protection, and the Bank, designated as national competent authority to ensure the compliance of Mastercard Europe with IFR Article 7, the bulk of which is devoted to "unbundling" requirements.

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 (NCBs), is in charge of the standard-setting process with regard to the oversight framework, as well as of 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 an 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 from representatives of the NCBs having a legitimate interest in overseeing the international CPS, the coordination of which being 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, established in Belgium, and for which the Bank ensures the role of overseer within the Eurosystem framework coordinating the assessment group.

The 2008 Eurosystem oversight framework for CPSs[1] has been revised to include the EBA guidelines on the security of internet payments and more specifically requirements relating to strong customer authentication. On this basis, a gap assessment of the CPS sector was started in 2016 and was finalised in the first half of 2018 in order to ensure that CPSs put in place all the necessary features enabling payment service providers (PSPs) (such as banks, PIs and ELMIs) to comply with the EBA guidelines. Due to their central position in processing card payments, it is crucial that CPSs' operations are designed in a way to make it possible for the PSPs to perform their roles of issuers and acquirers in compliance with all existing legal rules, industry best practices and existing standards. Each CPS performing operations in the euro area[2], be they domestic or international ones, has been covered by the gap assessment. During the last quarter of 2018, the Bank monitored the measures put in place by the CPSs following the recommendations issued at the end of the gap assessment process with regard to the EBA guidelines on the security of internet payments. Similarly, close contacts have been maintained in order to ensure that the CPSs stay on track in effectively implementing measures to accommodate in due time the requirements in the field of strong customer authentication as imposed on the PSPs by PSD2.

In this context, the Bank conducted on a solo basis the assessment of Bancontact, whereas for Mastercard Europe, the Bank coordinated the activities of the Eurosystem assessment group in charge of this international CPS. The ECB compiled all individual gap assessment reports, both for domestic and international CPSs (16 in total), enabling a full view of the sector's compliance with the EBA guidelines on the security of internet payments. An anonymised version of this global gap assessment report was published on 17 September 2018[3]. As general conclusion,

1 Eurosystem Oversight Framework for Card Payment Schemes – Standards (January 2008) and Guide for the assessment of card payment schemes against the oversight standards (February 2015).

2 Above the minimum threshold set in the Eurosystem Oversight Framework for Card Payment Schemes – Standards (January 2008).

3 Eurosystem report on the gap assessment of card payment schemes against the "Oversight framework for card payment schemes – standards"
https://www.ecb.europa.eu/pub/pdf/other/ecb.Eurosystem_report_on_the_gap_assessment_of_card_payment_schemes_2018.pdf?118ac6c691a3b08ee55ec74544dfa187

11 CPSs were reported to fully observe all oversight standards while the remaining five observe them broadly. Observance levels of CPSs were lowest for the standard on security, operational reliability and business continuity, whereby the most significant findings were made in the area of security risk management and transaction-related security aspects (e.g. customer authentication procedures, safeguarding security credentials or cryptographic material). On the other hand, measures to monitor all transactions processed and block potentially fraudulent ones have been implemented by many schemes.

In July 2018, the domestic scheme Bancontact merged with the mobile payment solution Payconiq and became Bancontact Payconiq Company. Both companies were (and the new company is too) owned by Belgian banks. For card payments, the scheme rules will remain unchanged: it continues to operate as previously and keeps its name as Bancontact. The merger will mostly have an impact on the mobile leg for which the card-based Bancontact app and the Payconiq mobile payment solution based on SCT (SEPA Credit Transfer) and SDD (SEPA Direct Debit) will be integrated in order to provide a unique mobile payment service called Payconiq by Bancontact.

The IFR requirement on the unbundling of scheme and processing activities within the same legal entity applies to Mastercard Europe and Visa Europe which are active in the whole EU. The designated national competent authorities (NCAs)[1] in each Member State that will assess/enforce the unbundling requirement for MasterCard Europe and Visa Europe have agreed that the Bank (for Mastercard Europe) and the UK Payment Systems Regulator (having supervisory competence for Visa Europe established in London) would table a joint proposal for cooperative monitoring of IFR compliance in that regard. The resulting MoU was signed at the end of 2018 by eight NCAs[2]. Other NCAs are expected to join the cooperative mechanism for monitoring the compliance with IFR Art. 7.1.a) at a later stage. The Bank has been formally designated by the signatory NCAs as lead NCA in charge of coordinating the cooperative working group devoted to Mastercard Europe[3]. In its capacity as NCA for Mastercard Europe, the Bank has already been informed by the latter about the effective measures put in place to comply with this Regulation.

The Bank also assessed whether Bancontact meets the requirements of IFR Art. 7.1.a). After due consideration given to the fact that the legal entity in charge of the scheme activities does not perform any processing activities, it can be concluded that Bancontact fully complies with the requirements of IFR Art. 7.1.a) and its associated RTS.

Oversight priorities in 2019

Regarding the cooperation mechanism for ensuring the compliance with IFR Art. 7.1.a), the effective monitoring tasks are expected to be engaged at the juncture of Q1 and Q2 2019. The target date for producing a monitoring/assessment report about the compliance of Mastercard Europe is scheduled for end of Q4 2019-Q1 2020.

With regard to the Bancontact – Payconiq merger, the Bank will continue to oversee the scheme and the oversight protocol will be updated in order to cover the new perimeter of the company.

In addition to its inclusion in the gap assessment from the perspective of internet payments, the cyber resilience of the CPS established in Belgium is now subject to further scrutiny from the angle of their use of and/or performance of tokenisation services[4].

1 IFR Article 13 stipulates that each Member State designates one or more competent authorities that are empowered to ensure enforcement of the IFR. In practice, such competent authorities can be e.g. central banks, supervisory bodies or any relevant public services entity.

2 NCAs designated by Belgium, Czech Republic, Denmark, Finland, Italy, Lithuania, the Netherlands and the United Kingdom.

3 The UK Payment Systems Regulator has been designated in the same role for Visa Europe.

4 In brief, tokenisation services include the generation of such tokens, as well their inclusion (and verification) in the card payment transaction process. The token itself is a surrogate of the payment card number (or PAN for Primary Account Number) and is aimed at replacing the latter throughout the payment chain at the level of the acquirer and merchant activities.