

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. 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 PSPs' environment in the country.

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, the European Real-time Gross Settlement (RTGS) system, is the large-value payment system connecting Belgian banks with other euro area banks for processing high-value 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 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.

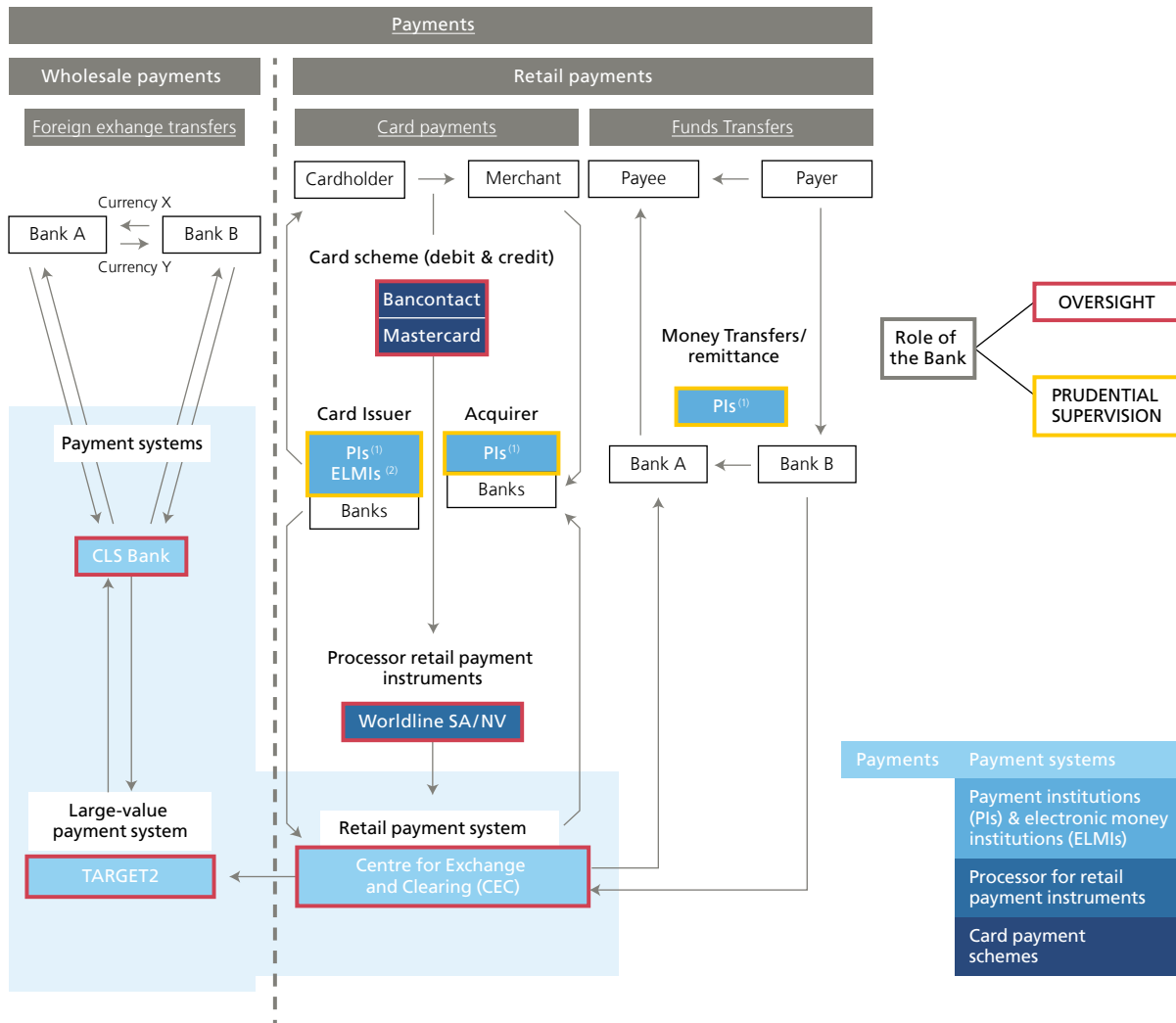
(1) A payment instrument is an instrument to execute payments such as cards, credit transfers and direct debits.

(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 3 SCOPE OF THE BANK'S OVERSIGHT AND PRUDENTIAL SUPERVISION ROLE IN PAYMENTS LANDSCAPE



Source: NBB.

(1) Payment institutions (PIs)

- Card acquiring and processing: Alpha Card, Alpha Card Merchant Services, Bank Card Company, B+S Payment Europe, Instele, Rent A Terminal, Worldline SA/NV
- Money Transfers/Remittance: Africash, Belmoney Transfert, Gold Commodities Forex, HomeSend, MoneyGram International, Money International, MoneyTrans Payment Services, Travelex.
- Direct Debit: EPBF
- Hybrid: BMCE EuroServices, Cofidis, eDebex, iBanFirst (before: FX4BIZ), Oonex, PAY-NXT, Santander CF Benelux, Cashfree, Ebury Partners Belgium, Teal IT

(2) Electronic money institutions (ELMIs)

- Buy Way Personal Finance, Fimaser, HPME, Imagor, Ingenico Financial Solutions, Ingenico Payment Services, Loyaltelk Payment Systems, RES Credit

Situation as of March 2018 covering Belgian PIs and ELMIs, as well as foreign entities with a branch in Belgium. In the course of 2017, licences for Belgian Money Corp, Munditransfers (PIs) and Orange Belgium (ELMIs) were withdrawn.

3.1 Payment systems

Oversight approach

The ECB is the lead overseer of TARGET2. The oversight is conducted on a cooperative basis with all the national central banks connected to TARGET2. In April 2017, the final comprehensive assessment reports for TARGET2, including the operators' proposed action plans to remediate the findings of the assessments (infringements and recommendations), were approved by the ECB's decision-making bodies. During the rest of the year the focus was on the follow-up to the assessment of the system as well as on the standard monitoring including new developments and risks. More detailed information on the oversight activities relating to TARGET2 oversight will be provided in the Eurosystem Oversight Report 2017 that is expected to be published later in 2018.

Regarding retail payment systems, the Bank is responsible for the oversight of the CEC. An assessment of the system against the ECB Revised Oversight Framework for RPS was conducted in the second half of 2016 as part of a Eurosystem-wide exercise and finalised in the beginning of 2017 after a peer review by the Eurosystem. This assessment concluded to the need for the system to reinforce and further develop its risk management function especially for operational and cyber risks. The system has now implemented measures aiming at correcting the weaknesses identified during this exercise.

In 2017, CEC's cyber resilience was also covered in the framework of the Bank's oversight activities. A Eurosystem-wide survey, based on a methodology developed for that particular purpose by the ECB and the NCBs, was conducted in order to assess the maturity of payment systems' controls in that field.

Complementary to its role of overseer of payment systems, the Bank is also competent authority for assessing the compliance of payment schemes established in Belgium with respect to Article 4 of the SEPA Regulation⁽¹⁾ on Interoperability. For the purposes of carrying out credit transfers and direct debits on behalf of participating PSPs, this Regulation requests payment schemes to be used by a majority of PSPs within a majority of Member States (the so-called interoperability condition). The new payment scheme called SEPA Instant Credit Transfer (or SCT Inst) launched by the European Payments Council (EPC) on 21 November 2017, and which is overseen by the ESCB, did not meet this condition on interoperability. Consequently, the Bank as competent authority for this aspect (as the EPC is formally established in Belgium) has granted the scheme a temporary exemption to the interoperability condition for a period of three years as provided for in Article 4(4) of this Regulation and after consulting the competent authorities in the countries launching the SCT Inst scheme. Over this three years period, the scheme is expected to develop into a fully-fledged payment scheme compliant with Article 4 of the SEPA Regulation.

Supervisory priorities in 2018

The CEC is currently developing a new functionality aiming at processing retail payments on a real-time basis, referred to as "instant payments", which is planned to be in place by November 2018. A specific platform used for the processing of those payments is developed by the French Automatic Clearing House operator STET jointly for the French and Belgian retail payments markets. A pre-assessment of this new functionality has been started in 2017 and will be conducted in cooperation with the Banque de France for issues relevant for both overseers.

The CEC's cyber resilience will be further examined by the Bank in 2018. This will be done jointly with the Banque de France which oversees STET. A cooperation framework between the Bank and the Banque de France, formalised in a Memorandum of Understanding (MoU), is in place in that context.

The measures implemented in 2017 by the CEC in order to correct the weaknesses identified during the assessment against the Revised Oversight Framework for RPS, in particular with regard to its risk management function for operational and cyber risks, will be assessed in 2018.

(1) Regulation (EU) No. 260/2012 of the European Parliament and of the Council of 14 March 2012 establishing technical and business requirements for credit transfers and direct debits in euro and amending Regulation (EC) No 924/2009.

3.2 Payment institutions and electronic money institutions

Changes in regulatory framework

Throughout the reporting year, the Bank has conducted preparatory work to implement the upcoming changes in the regulatory framework for the entry into force of PSD2⁽¹⁾. The key aim of the amended Directive, which applies as of 13 January 2018, is to stimulate both innovation and competition in the payments market by further harmonising current rules and expanding the scope of regulation to new digital payment services, while keeping abreast of adequate security levels.

In line with these objectives, PSD2 adds two important novelties to the current legislation. First of all, the scope of the PSD1 is enlarged through the inclusion of new types of services that will be regulated: payment initiation services and payment account information services. It implies that, *account servicing payment service providers* (ASPSPs), such as credit institutions and certain PIs or ELMIs, are obliged to open up the access to the payment accounts they maintain for payment service users. This *open* access to payment accounts can subsequently be used by third-party providers, known as *payment initiation services providers* (PISPs) and *account information service providers* (AISPs), provided they obtain the prior explicit consent of the payment service user and are authorised by their national competent authority (in Belgium, the Bank). As such, the PSD2 allows for example for third-party providers to aggregate a user's account information from different payment accounts into one application. Chart 4 provides a schematic overview of business processes related to these new payment services post-PSD2 as well as their providers.

A second important change is directly linked to the new type of payment services and the development of regulatory technical standards (RTSs)⁽²⁾ regarding updated and advanced security requirements⁽³⁾. As a new category of institutions will be granted access to bank accounts (always after the explicit consent of the payment service user/account holder), strong security measures need to be in place to avoid malpractice. Therefore, an important novelty with regards to the PSD2 relates to the development of updated security requirements and the obligation to apply *strong customer authentication*⁽⁴⁾ when initiating and executing payments by PSPs. RTSs have been developed on both the application of strong customer authentication, and the exemptions therefrom, and on the requirements related to the *common and secure open standards of communication* that needs to be established between third-party providers and ASPSPs when the former initiates a payment or seeks access to account information⁽⁵⁾. Furthermore, the Guidelines on the authorisation of PIs aim to harmonise the requirements to which firms need to comply if they wish to obtain an authorisation from a national competent authority⁽⁶⁾.

Prudential and oversight approach

The Bank is the national competent authority within Belgium for prudential supervision on 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 stringent authorisation requirements than a *full* licence, is to allow startups and small institutions to

(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 development of the related RTSs takes place within the broader mandate given by the European Commission to the European Banking Authority (EBA) to safeguard the European-wide harmonisation and implementation of PSD2. RTSs cover the Directive adopted by the European Parliament and the Council and are binding in national regulatory frameworks. They have to be submitted to the European Commission for endorsement by means of delegated or implementing acts. Guidelines on the other hand can also be addressed to competent authorities, or market participants, but do not have to be endorsed by the European Commission. Competent authorities have to comply with these or publish their reasons for non-compliance.

(3) Several other mandates to develop RTSs were relayed by the European Commission to the EBA. They include the following aspects: the harmonisation of templates for passport notifications, the classification of major incidents and the mechanisms through which these need to be reported, the types of fraud statistics to report, the type of operational and security risk framework PSPs need to establish, the calculation method of the minimum monetary amount of the professional indemnity insurance PSPs need to hold and the mechanisms through which complaints need to be handled.

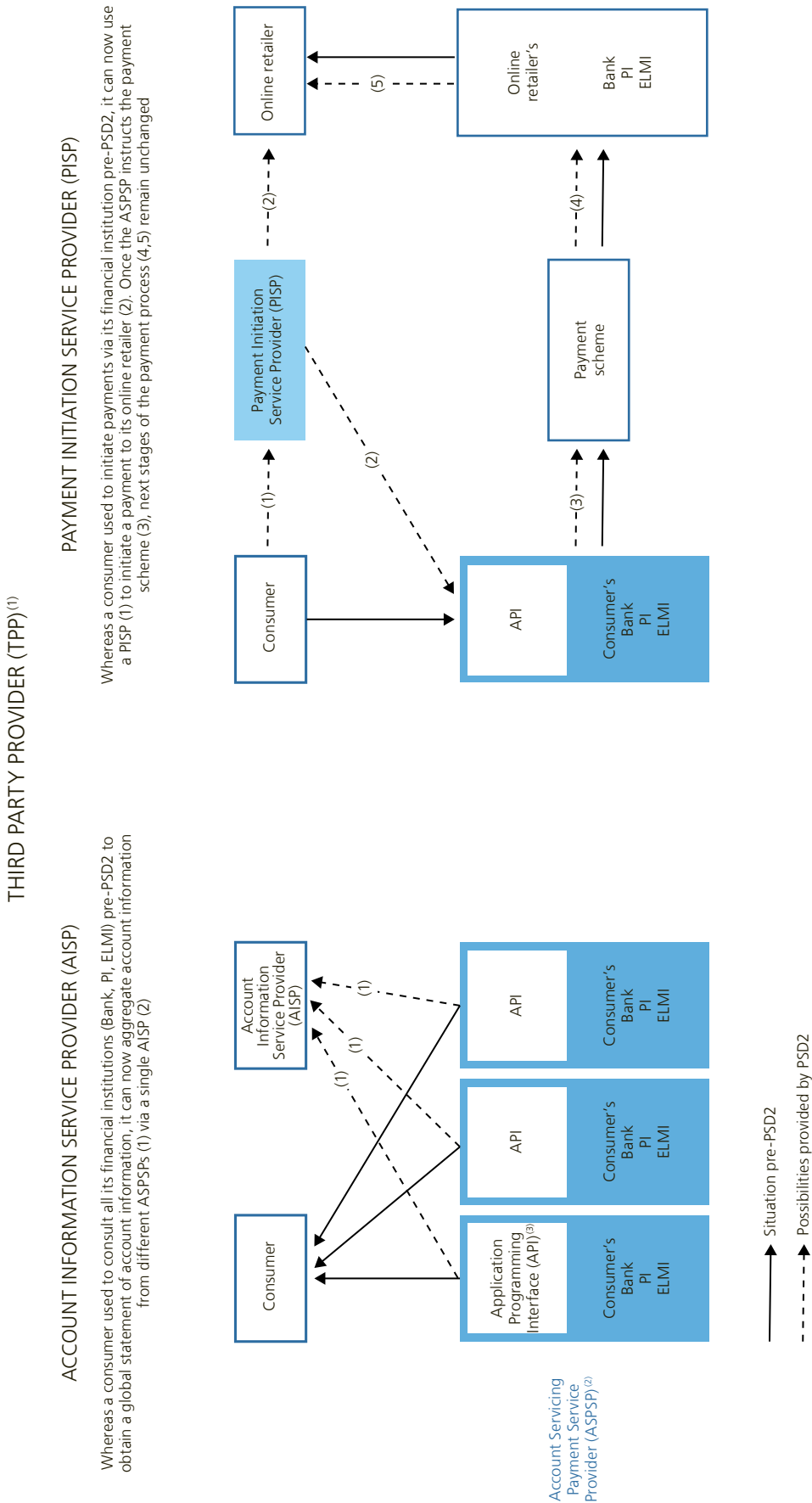
(4) Article 4(30) of the PSD2 defines strong customer authentication as an authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inference (something the user is) that are independent, and is designed in such a way as to protect the confidentiality of the authentication data.

(5) https://eur-lex.europa.eu/resource.html?uri=cellar:e3e13b98-da05-11e7-a506-01aa75ed71a1.0016.02/DOC_1&format=PDF.

(6) EBA Guidelines under Directive (EU) 2015/2366 (PSD2) on the information to be provided for the authorisation of payment institutions and e-money institutions and for the registration of account information service providers, EBA/GL/2017/09, 11 July 2017. See also: <https://www.eba.europa.eu/documents/10180/1904583/Final+Guidelines+on+Authorisations+of+Payment+Institutions+%28EBA-GL-2017-09+%29.pdf>.

CHART 4

SCHEMATIC OVERVIEW OF BUSINESS PROCESSES RELATED TO NEW PAYMENT SERVICES AND THEIR PROVIDERS



(1) **TPP (Third Party Provider)**: a TPP can be (1) a **PISP (Payment Initiation Service Provider)**, licensed by the Bank and subject to a lighter prudential regime of the Bank (as no access to clients' funds) or (2) an **AISP (Account Information Service Provider)**, registered by the Bank (no access to clients' funds). TPPs can be banks, PIs or ELMIs.

(2) **ASPSP (Account Servicing Payment Service Provider)**: banks, PIs or ELMIs supervised and licensed by the Bank.

(3) **API (Application Programming Interface)**: dedicated application interface per service.

enter the market relatively quick to be able to launch their product or service fostering both innovation and competition. The regime, which is optional for Member States, requires firms to apply for a full authorisation once they reach a certain threshold. As long as firms 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 adapted in the Belgian Law of 11 March 2018 reducing the applicable thresholds for PIs and ELMIs⁽¹⁾.

A specific application procedure has been established by the Bank for institutions that seek to relocate their activities to Belgium. The scope of this particular procedure is strictly limited to PIs and ELMIs which have already obtained a licence in another EEA Member State and which effectively envisage to move their payment service or e-money operations to Belgium. In 2017, the Bank authorised two firms, MoneyGram International SPRL and Ebury Partners Belgium NV. The relocation of these two firms from the UK to Belgium will impact the supervisory activities conducted by the Bank, as both firms have operations throughout the EEA. Box 5 provides an overview of the sector of PIs and ELMIs.

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

Box 5 – Sector of payment institutions and electronic money institutions in Belgium

New actors such as payments institutions (PIs) and electronic money institutions (ELMIs) are entering the market of payment services which used to be dominated by banks. This trend is due to several factors such as the revised Payment Services Directive (PSD2) and technological changes leading to new types of payment services.

As of end 2017, there were 24 PIs and 8 ELMIs in Belgium. As illustrated in chart 1 below, the number of PIs has increased gradually while for ELMIs, fewer initiatives were launched in the last few years. PIs and ELMIs are subject to prudential supervision by the Bank. If the value of payment transactions does not exceed a threshold amount, these institutions can be subject to a “waiver” regime providing less stringent requirements on the minimum capital levels, as well as on the reporting procedure and internal control mechanisms. End 2017, the threshold amount was set at € 3 million of transactions per month on average for PIs and € 5 million of outstanding e-money for ELMIs. At that time, five PIs and three ELMIs operated under such waiver. The implementation of the Law of 11 March 2018 transposing the PSD2 reduced the threshold for PIs to € 1 million and the one for ELMIs to € 1.5 million.

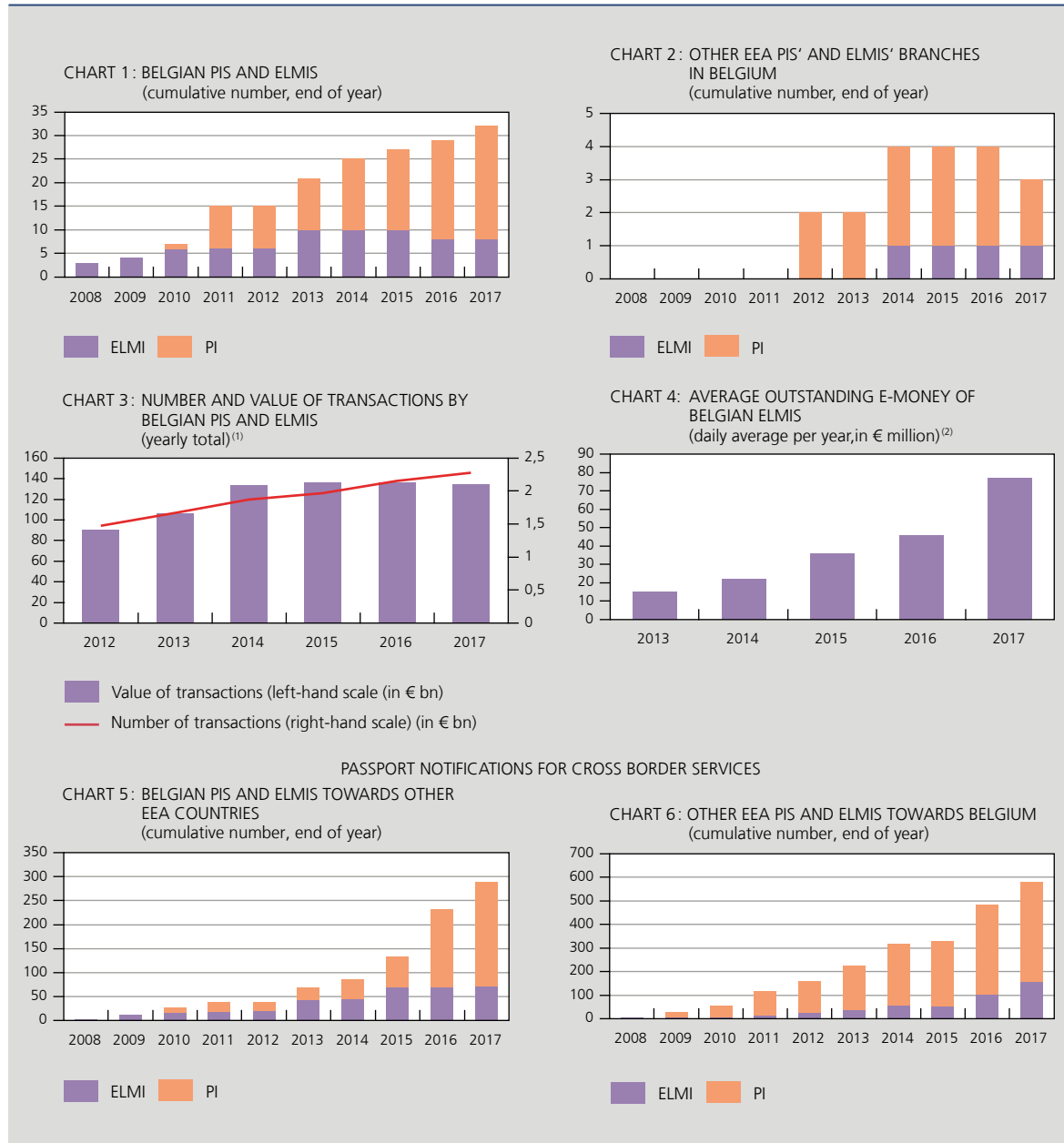
PIs and ELMIs that have a licence in a EEA Member State can develop cross-border services either by setting up a local branch or by passporting services, with or without an agent network. PIs and ELMIs establishing a branch in another Member State can provide the same services as they offer in their home country. While there is only one Belgian PI (iBanFirst) having a branch in another EEA Member State, chart 2 shows that, as of end 2017, there are three EU branches in Belgium (PIs Santander Consumer Finance and BMCE, and ELMI Ingenico Payment Services). The supervisor of the home country of these institutions remains responsible for prudential supervision. Branches have a limited reporting obligation towards the Bank as host country supervisor. The Bank is only responsible for rules of general conduct, in particular anti-money laundering requirements.

In terms of activity, the monthly average number and value of transactions processed by Belgian PIs and ELMIs is covered in chart 3. The number of transactions rose with more than 50 % in the course of 2012-2017, whereas the value of transactions increased with more than 30 % although the amount is more or less stable in the last few years. Chart 4 shows that the average outstanding e-money of Belgian ELMIs stood end 2016 at about € 45 million which – although three times higher than in 2013 – is still a relatively small amount.



Passporting services in other EEA Member States is a second way to develop cross-border activities. Total of passport notifications of cross-border services of Belgian PIs and ELMIs has increased significantly. For 32 Belgian PIs and ELMIs, there are respectively 218 and 72 passport notifications, mainly to neighbouring countries (chart 5). There are also 421 foreign PIs and 156 ELMIs from another EEA Member State that were notified as providing

EVOLUTION OF THE SECTOR OF PIS AND ELMIS IN BELGIUM



Source: NBB.

(1) Yearly totals calculated based on monthly average number and value of transactions. Data exclude transactions processed by PIs and ELMIs operating under a "waiver" regime and branches of EEA PIs and ELMIs in Belgium.

(2) ELMI reporting obligation as from 2013.

services in Belgium (chart 6). More than half of these institutions have residence in the UK which is currently the prime host of PIs and ELMIs in the EU. Supervisors among EEA countries exchange information that entails notification of new institutions, closures and changes in the agent network of these institutions.

A third way to provide cross-border services is passporting payment services in other EEA Member States via an agent network (or distributor network in the case of ELMIs). This option is used by four Belgian PIs (Travelex, Moneytrans Payment Services, Worldline and Moneygram). As of end 2017, there were 823 agents in total (most of them representing Moneytrans and active in Italy as host country), but as Moneygram – having obtained its license end of 2017 – will migrate its agent network as well, the number of agents of Belgian PIs will rise to more than 10 000 in the course of 2018. Similarly, three Belgian ELMIs (HPME, Imagor and Ingenico Financial Solutions) also rely on such an agent/distributor network (most of them representing HPME and active in France as host country). For these agents of Belgian PIs and ELMIs, the Bank performs a fit & proper analysis, in accordance with the law of 21 December 2009.

Foreign based PIs and ELMIs can also passport their services in Belgium via an agent/distributor network. End 2017, 23 PIs (out of 421) had about 2100 agents (in particular money remitters). Similarly, out of 156 ELMIs, five offer their services via (11) distributors/agents. These agents (or distributors) are being notified to the Bank and have to comply with the anti-money laundering reporting. All other supervisory responsibilities remain with the supervisor of the home country.

Supervisory priorities in 2018

In March 2018, the PSD2 was transposed into Belgian law repealing and replacing the Law of 21 December 2009 transposing PSD1. The Bank's supervisory activities on PIs and ELMIs are driven by the regulatory changes brought by PSD2. Institutions authorised under PSD1 need to submit all relevant information to their competent authorities to allow them to assess, by 13 July 2018, whether those institutions comply with the new requirements laid down in the PSD2 and, if not, which measures need to be taken in order to ensure compliance, or whether a withdrawal or the authorisation is appropriate. Therefore, all licensed PIs and ELMIs in Belgium have to be re-authorised and they have introduced (or are in the process of introducing) transition files demonstrating their compliance with PSD2. The Bank will assess the re-authorisation of each currently authorised PI or ELMI in the first half of 2018 by focusing on, among others, whether an appropriate incident reporting mechanism is installed or whether the required security policies are in place. Furthermore, new applicant institutions (and institutions wishing to relocate to Belgium) should introduce an application file to the Bank.

The new regulatory framework requires the Bank to develop, among others, revised circulars and reporting tools to monitor compliance with the updated requirements mandated by the PSD2. Moreover, the RTS and guidelines, developed by the EBA under the mandate of the European Commission and fully applicable in Belgium, also require the Bank to communicate and enforce these with the Belgian payment services industry.

Another supervisory priority in 2018 consists of implementing the Bank's prudential approach towards newly authorised institutions, such as third-party providers. The revised regulatory framework mandates several new security requirements for these actors. These include for example the disposition that personalised security credentials have to be transmitted through safe and efficient channels. Furthermore, the communication between third-party providers and the payment account at the ASPSP includes the use of a dedicated interface, which must be made available by the ASPSPs and must comply with the security requirements of ISO20022, the international standard for financial communications. To reinforce security with regard to payment services provided via third-party providers, the use of this interface is mandatory from the entry into force in September 2019 of the RTS on strong customer authentication and on common and secure open standards of communication. The dedicated interface will be provided by ASPSPs by so-called APIs (Application Programming Interfaces), whereby the communication and transfer of data between the ASPSPs and the third-party providers is ensured. 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.

The Bank will continue to participate in the international work done by the European Commission and EBA to ensure a common and harmonised European approach with regards to the implementation of PSD2.

Lastly, the Bank aims to further strengthen the bilateral dialogue with the sector of FinTech companies and start-ups, including through its contact point set up in cooperation with FSMA (see box 6).

Box 6 – FinTech single point of contact

In view of the growing interest from the market for innovation in financial technology (FinTech), the Bank and the FSMA, decided to set up a single point of contact. It acts as a unique access point for Fintech start-ups, or any other firm or person, providing guidance on the regulatory qualification of planned activities, for the licence application process and the regulatory framework⁽¹⁾. Since its launch in April 2017, several questions were received, ranging from the legislative framework for the provision of payment services to the creation of online exchange offices for virtual currencies. While the interest in virtual currencies has increased as well, questions mainly concern the legislative framework for the provision of payment services⁽²⁾.

Based on anecdotal evidence from FinTech companies and start-ups, one can argue that significant investments at the initial stage are necessary, often requiring a substantial amount of available capital to obtain a sufficient level of scale. Whereas scale is considered to be a pre-requisite for turning to profitability, there are a number of obstacles to expand activities and attracting a larger number of users. Such obstacles include the implementation of appropriate internal control systems (especially if a limited number of employees is available) and poor familiarity with the new regulatory framework for payment services. On the other hand, access to funding is not perceived by Fintech companies and other start-ups as problematic as such (although it presumes they have a realistic idea about the amount of capital needed to generate profit eventually).

(1) <https://www.nbb.be/en/financial-oversight/general/contact-point-fintech>.

(2) 45 questions were received in the FinTech mailbox between April 2017 and January 2018, whereof 11 questions concerning virtual currencies and 28 concerning payments.

3.3 Processors of payment transactions

Changes in regulatory framework

The proper functioning of payment systems processing is a primary objective of the oversight of payment systems. With respect to payment instruments, card schemes and their processing, the Bank's enforcement of oversight standards and requirements has evolved into hard-law-based oversight for systemically relevant payment processors (entities within the scope of the Law of 24 March 2017 on the oversight of payment transactions processors⁽¹⁾). The new law has significantly strengthened the enforcement of the applicable oversight standards⁽²⁾ on all payment processors that are considered systemically relevant in the Belgian payment transactions market, regardless of where such processor has its registered office.

(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) The applicable oversight requirements of the Law of 24 March 2017 on processors of payment transactions are derived from the 2012 CPMI-IOSCO Principles on Financial Market Infrastructures, notably Principles 2 (Governance), 3 (Framework for the comprehensive management of risks) and 17 (Operational risk).

Prudential and oversight approach

Worldline SA/NV is the Belgian entity of the Worldline group which is, on its turn, part of the French IT service group Atos (see also Annex 2). Worldline SA/NV has systemic relevance from an oversight perspective since it has a significant position in the processing of Belgian debit and credit card payments. It has therefore been designated as a systemically relevant payment processor under the Law of 24 March 2017. The role of cards as payment instruments in Belgium, and Worldline SA/NV's role in it, is covered in box 7.

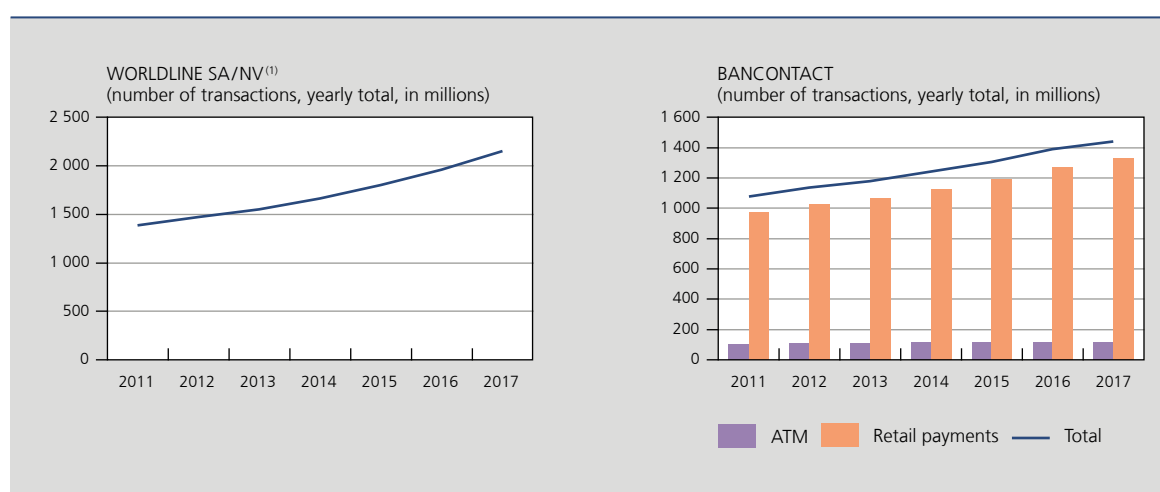
Following the investment of the Worldline Group in Equens SE (NL), which entailed the contribution in kind of Worldline SA/NV's processing business unit in the Dutch Automated Clearing House, Equens subsequently changed its name to equensWorldline SE. Its activities encompass the operation of the Dutch Automated Clearing House as well as the processing of payments operations as a service provider for the different Worldline entities. Only payment processing activities that equensWorldline SE performs for Worldline SA/NV are within the scope of the Bank's oversight. Its other payment processing and clearing activities are out of scope. equensWorldline SE has, together with Worldline SA/NV, been designated as a systemically relevant payment processor under the Law of 24 March 2017 for the processing activities it performs as a service provider to Worldline SA/NV and falls therefore under the hard-law based direct oversight of the Bank.

Prior to the establishment of equensWorldline SE, an on-site inspection was conducted by the Bank at Worldline SA/NV covering the company's operational risk management and operational risk governance. Based on the conclusions of this exercise, a follow-up inspection was conducted in the course of 2017 to assess the adequacy of the implemented measures.

Box 7 – The role of cards as payment instrument in Belgium

Different instruments can be used by consumers to make payments in Belgium; i.e. card payments, credit transfers, direct debits, e-money, cheques, and, obviously, cash. Worldline SA/NV is the main processor of payment transactions in Belgium. Throughout 2017 it processed more than 2 billion transactions in total, about 55 % higher

CARD TRANSACTIONS IN BELGIUM



Source: Worldline SA/NV, Bancontact.

(1) Worldline operations include card payments (Bancontact, Maestro, Visa, Mastercard, Union Pay, JCB etc.) in Belgium (for Belgian cards holders and cards issued abroad) and abroad (for cards issued in Belgium), at POS and ATM.

than in 2011 (see chart below, left-hand panel). A very large part of them are processed by Worldline SA/NV on behalf of the domestic card scheme Bancontact, followed by credit card (VISA, Mastercard) and other transactions (Maestro, etc.). The number of Bancontact transactions equaled about 1.4 billion in 2017 of which 8 % related to ATM operations. Compared to 2011, the number of transactions in 2017 was 34 % higher; ATM transactions increased with 13 %, whereas retail payments with more than 36 % (right-hand panel).

Supervisory priorities in 2018

Considering its systemic importance as payment processor in Belgium, cyber resilience is key for a company like Worldline SA/NV managing an extended Information Technology Center network for making card payments. The Bank will pay specific attention to the cyber resilience of Worldline SA/NV and will also, where needed, further detail the requirements of the law of 24 March 2017 on the oversight of payment operations processors.

3.4 Card payment schemes

Changes in regulatory framework

Under Article 7.1 (a) of EU Regulation 2015/751 on interchange fees for card-based payment transactions (IFR)⁽¹⁾, when payment card scheme governance activities (i.e. rules, licensing, business practices) and payment transaction processing activities (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) 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⁽²⁾ based on which the national competent authorities are going to 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 (1) accounting (separated profit and loss accounts with transparent allocation of expenses and revenues, annual review by an independent and certified auditor of the financial information reported to the national competent authorities), (2) organisation (a.o. via two separate internal business units located in separate workspaces with restricted and controlled access, distinct remuneration policies, no sharing of sensitive information) and (3) decision-making process (separate management bodies for the scheme and processing business units, separate annual budget plans).

Based on the IFR, supervisory tasks have been divided between the Belgian Federal Public Service for the 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 on unbundling.

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.

(1) 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.

(2) 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.

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 gap assessment report is then peer reviewed by representatives of other Eurosystem NCBs before being submitted to the ECB. The monitoring of ongoing compliance is also 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 CPSs sector was started in 2016 (and is expected to be finalised in the course of 2018) in order to ensure that CPSs put in place all the necessary features enabling 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.

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. After peer reviews by respectively other Eurosystem NCBs and members of the assessment group, the assessment reports were provided to the ECB in mid-January 2018. The ECB will compile all individual gap assessment reports, both for domestic and international CPS, enabling to have a full view of the CPS sector's compliance with the EBA guidelines on the security of internet payments. An anonymised version (without individual CPS names) of this global gap assessment report is scheduled to be published by the ECB at the end of the second quarter of 2018.

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 EU as a whole. The designated national competent authorities⁽³⁾ 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 competences regarding Visa Europe established in London) would table a joint proposal for cooperative monitoring of IFR compliance in that regard. Together with the UK Payment Systems Regulator, during the course of 2017, the Bank started to establish the arrangements based on which national competent authorities shall cooperate on a voluntary basis to monitor the implementation of the unbundling requirements of IFR. The resulting MoU with other relevant designated national competent authorities is expected to be signed in the course of 2018.

Oversight priorities in 2018

Based on the forthcoming MoU with interested national competent authorities, the Bank will start the effective monitoring of the unbundling of scheme and processing activities as required in the RTS published in January 2018. In addition, the Bank will also, where needed, monitor (i) the implementation of the recommendations addressed to the CPSs at the end of the gap assessment process and (ii) the initiatives of CPSs to evolve towards a mandatory use of strong customer

(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) 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.

authentication, which is the core element of the EBA guidelines for the security of internet payments. In that regard, Mastercard requires, well ahead of the finalisation of the gap assessment, all European issuers and acquirers and online merchants to implement mandatorily strong customer authentication requirements (stemming from PSD2 and related RTS) between April and July 2019. Although already covered in the gap assessment from the perspective of internet payments, the cyber resilience of the CPSs established in Belgium will be further analysed and monitored by the Bank.