Financial Market Infrastructures and Payment Services

Report 2018

National Bank OF BELGIUM

Eurosystem

The Financial Market Infrastructures and Payment Services report is the result of a collective effort. The following people have actively contributed to this issue of the report:

N. Boeckx, K. Bollen, B. Bourtembourg, F. Caron, P. Gourdin, J. Jans, I. Meau, L. Ohn, S. Siedlecki, C. Stas, R. Temmerman, M. Van Acoleyen, S. Van Cauwenberge, J. Vermeulen

Contents

Introduction and executive summary

This is the second edition of the Bank's Financial Market Infrastructures and Payment Services Report. It covers a wide range of financial market infrastructures (FMIs), custodians, payment service providers and critical service providers for which the Bank is responsible for prudential supervision or oversight, either as lead authority or in cooperation arrangements with other authorities. Although these systems and institutions may differ in scope and size – some of them have international systemic relevance – they all serve as the backbone for processing payments between individuals and/or financial institutions, securities transfers or messages on behalf of participants and/or clients. Therefore, their safe, sound and efficient functioning is one of the priorities of the Bank's supervisory and oversight activities.

The risk environment is evolving and becoming more complex. While physical security risk was a major concern after 9/11, and liquidity risks were one of the main focuses in the aftermath of the Lehman debacle, digital security (including data integrity) dominates risk management agendas today, not least because of a series of cyber heists in the last few years. The Bank is closely monitoring efforts made by the sector of FMIs and payment services to implement the CPMI-IOSCO cyber security guidance. The interconnectivity with other systems, institutions and participants, at wholesale or retail level, adds to the complexity of operational and cyber risks and to the potential impact. Also, the level of interconnectedness in the financial sector can evolve over time. On a longer term, new technologies like blockchain have the potential to lead to a certain degree of disintermediation. In other cases, regulatory initiatives such as the revised EU Payment Services Directive (PSD2) pave the way for the introduction of new stakeholders. With the aim of fostering competition, facilitating and regulating new core services for payment accounts, payment service providers (for the time being mainly banks) are required to open up access to their bank accounts to new categories of regulated institutions (if the bank account holder wishes to do so). This provides access for new, licensed suppliers providing new services using bank account data, which were until now in the remit of the traditional players (banks). Access to and storage of such sensitive (payments) data requires appropriate risk management.

As a rule, a chain of actors (connected systems, institutions and their participants or clients) is as strong as the weakest link between the nodes. Participants/clients, sometimes at the periphery of the network, are part of the so-called endpoints in the payment chain. The article on endpoint security strategies to mitigate payment fraud builds further on the CPMI report on wholesale payments security. It covers and compares strategies sponsored by different stakeholders in different areas of the sector of FMIs and payment services. As payment system operator, the central bank community itself should implement these endpoint security strategies, whereas in its role as supervisor or as catalyst, it should monitor and promote implementation in privately operated systems.

Like last year, the Report covers changes in the regulatory environment, as well as the Bank's oversight and prudential supervisory approaches, and its main priorities for 2018. In addition, the Report zooms in on specific themes such as developments in the sector of payment institutions and electronic money institutions, the role of cards as payment instrument in Belgium, while for other systems or institutions specific information is provided on their international dimension. As the Report is intended as a reference document, annexes on applicable rules/principles and statistics provide further insight for those interested.

1. The Bank's role in oversight and prudential supervision of financial market infrastructures, custodians, payment service providers and critical service providers

To provide more insight in the systems and institutions providing payment, clearing, settlement, custody and other services, either from a wholesale or a retail market perspective, section 1.1 provides an overview of the structure and interdependencies between them. Relevant processes and flows are more explained in detail in the next parts of this Report (i.e. chapters 2, 3 and 4). Section 1.2 explains the Bank's mandate and role in the oversight and prudential supervision of this sector, either on a national or international basis.

1.1 Critical nodes in the functioning of financial markets and payment services

The systems and institutions covered in this Report can be ranked in three categories according to the type of service provided : (i) securities clearing, settlement and custody, (ii) payments and (iii) critical service providers to the financial infrastructure. Through their activities or services provided to the financial industry, these systems and institutions are the critical nodes in the functioning of financial markets and payment services as well as the real economy. If designed safely and managed properly, they are instrumental in reducing systemic risks and contagion in the event of financial crisis. At the same time, they are interlinked with FMIs, financial intermediaries and other actors such as merchants or retail customers. These interdependencies are briefly presented below and illustrated in chart 1

Securities clearing, settlement and custody

A trade in a financial instrument is concluded between a buyer and a seller by agreeing the price and the contract terms. Trading can be on-exchange (i.e. on a centralised platform designed to optimise the price-discovery process and to concentrate market liquidity) or bilaterally on an over-the-counter (OTC) basis (i.e. where the counterparties make the bid and accept the offer to conclude contracts directly among themselves). In both cases, buyer or seller are usually banks or investment firms. They could rely on other intermediaries (e.g. brokers) to conduct trades. Trade exchanges such as Euronext Brussels are supervised by securities regulators and are not covered in the Report.

FMIs and financial institutions that provide securities clearing, settlement and custody services are considered part of the post-trade securities landscape. The clearing of a trade via a central counterparty (CCP) generally means that the CCP becomes the buyer counterparty for the seller and the seller counterparty for the buyer. Both original counterparties to the trade then have a claim on the CCP. The direct participant of a CCP – usually a bank or an investment firm – is called a clearing member. A clearing member may clear not only its own trades via the CCP, but also those of its clients.

Whereas there are no CCPs established in Belgium, CCPs in other countries can be systemically important due to their clearing activities for the Belgian securities market.

After clearing, the settlement of a trade results in the transfer of cash and/or of a financial instrument between the parties in the books of a central securities depository (CSD). CSDs generally act as the register of securities issued in their domestic market. In the case of international securities, such as Eurobonds, issuers can choose the currency or country of issue. These securities are held in international CSDs (ICSDs)[1]. When a CCP has intervened to clear a trade, settlement takes place on the books of (I)CSDs[2] between the buyer and the CCP, and between the seller and the CCP. There are three (I)CSDs established in Belgium: Euroclear Bank (ICSD), Euroclear Belgium and NBB-SSS (both CSDs). The cash leg of securities settlement takes place either in payment systems operated by central banks (i.e. central bank money, for example TARGET2) or on the books of an (I)CSD with banking status providing (multicurrency) cash accounts (i.e. commercial bank money, for example Euroclear Bank).

Financial institutions that facilitate their clients' access to securities investment markets are referred to as custodians. In that capacity of intermediary, custodians can offer their clients safekeeping and settlement services. A local custodian primarily focuses on serving a single securities market. If a custodian has access to multiple markets, it is considered a global custodian. The Bank of New York-Mellon SA/NV (BNYM SA/NV), established in Belgium, is the global custodian of the BNYM group providing investment services to more than 100 securities markets.

Payments

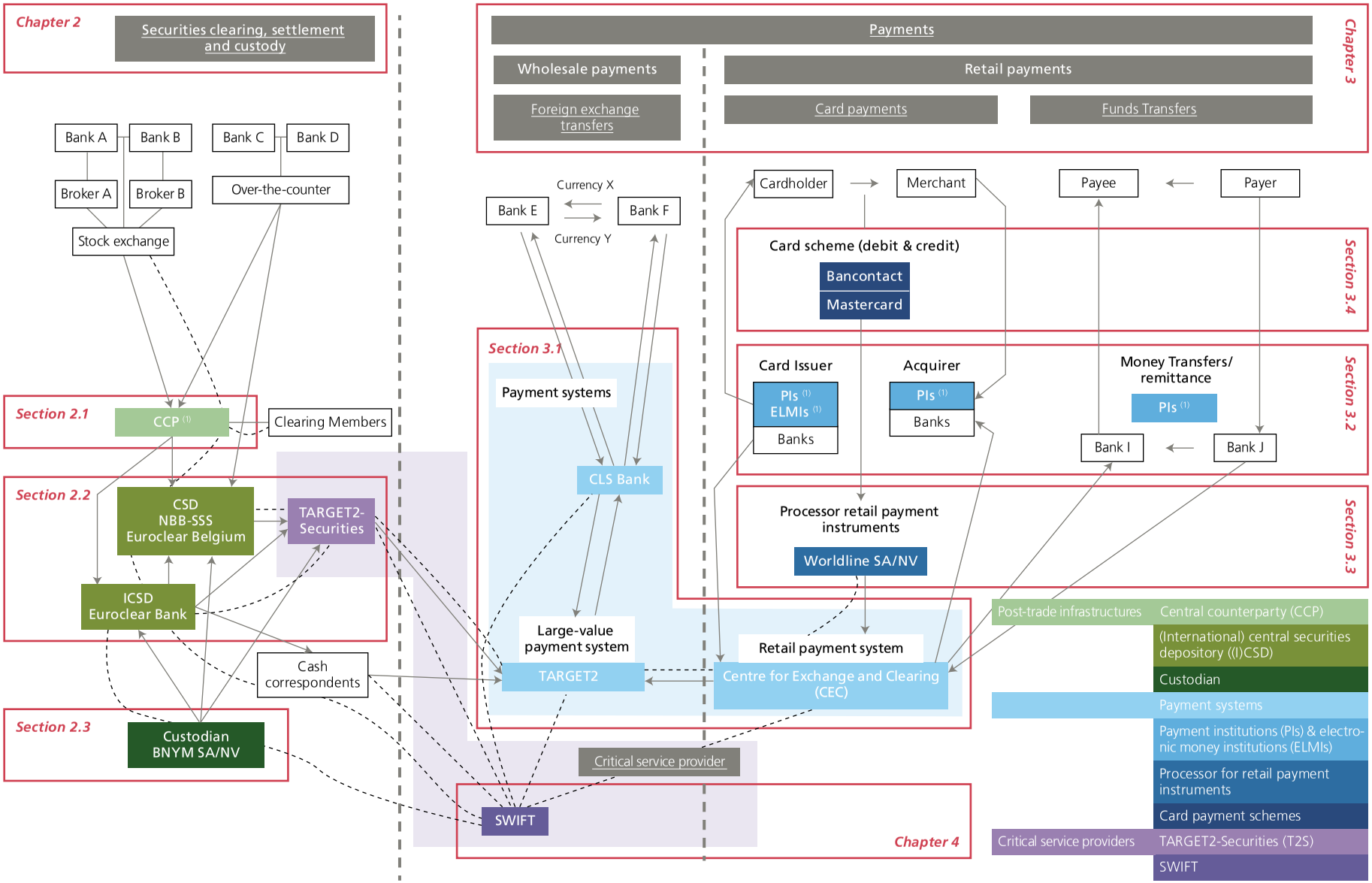
The payments landscape covers both wholesale (i.e. transactions between institutional investors) and retail payments segments (i.e. transactions between retail customers), and includes payment systems, payment service providers (PSPs) such as payment institutions (PIs) and electronic money institutions (ELMIs), processors of payment transactions and card payment schemes.

Payment systems cover both large-value payment systems (LVPS) and retail payment systems (RPS). While LVPSs generally exchange payments of a very large amount, mainly between banks and other participants in the financial markets, RPSs typically handle a large volume of payments of relatively low value such as credit transfers and direct debits. In Belgium, most payments are processed by TARGET2, the large-value payment system connecting Belgian with other European banks, and by the Centre for Exchange and Clearing (CEC), which is the domestic retail payment system processing intra-Belgian domestic payments.

Card payments typically involve a "four-party scheme", i.e. cardholder, card issuer, merchant and acquirer. The card of the person on the purchase side of a transaction (cardholder) with a merchant is issued by an institution (card issuer) which was traditionally always a bank, but can, nowadays, also be a PI or ELMI. The acquirer is in charge of acquiring the transaction on behalf of the merchant (i.e. performing for the merchant all the steps necessary for the buyer's money to be paid into the merchant's account). The role of PIs and ELMIs in the retail payments area is multiple. For instance, in the case of card payment transactions, PIs and ELMIs can issue the payment cards to the user and/or acquire the funds for the payment on behalf of the merchant. The acquiring business has gradually become a market whereby, alongside banks, PIs are playing a growing role. The relevant rules and features according to which card payments – either debit or credit – can take place are defined by card payment schemes. The Belgian domestic (debit) card payment scheme is Bancontact. Mastercard Europe (MCE) is an international (credit) card payment scheme established in Belgium. One processor provides the underlying network and services for virtually all card payments, namely Worldline SA/NV. After processing card payments, transactions are sent to the CEC for clearing and settlement. As well as card payments, PIs have a major role in providing money transfer/remittance services (fund transfers) allowing retail customers to transfer cash from Belgium to a third party in different locations around the world and vice versa.

(1) In this case, a duopoly exists as there are two ICSDs in the EU which act as "issuer CSD" for Eurobonds; i.e. Euroclear Bank established in Belgium and Clearstream Banking Luxembourg.
(1) The term (I)CSD is used to cover both CSDs and ICSDs.

CHART 1 INTERLINKAGES THROUGH & BETWEEN FINANCIAL MARKET INFRASTRUCTURES, CUSTODIANS, PAYMENT SERVICE PROVIDERS AND CRITICAL SERVICE PROVIDERS



Source: NBB.
(1) Individual institutions are listed in Table 1.

CLS Bank, a US-based settlement system for foreign exchange (FX) transactions is linked to the LVPS systems operated by central banks of 18 currencies (including TARGET2 for EUR), making it possible to settle both legs of the FX transaction at the same time. CLS Bank eliminates FX settlement risk when – due to time zone differences – one party wires the currency it sold but does not receive the currency it bought from its counterparty.

Critical service provider

TARGET2-Securities (T2S) and SWIFT are considered critical service providers in this Report. T2S is the common settlement platform for European CSDs. Although SWIFT is neither a payment system nor a settlement system, a large number of systemically important systems depend on it for their daily financial messaging.

1.2 FMIs, custodians, payment service providers and critical service providers subject to oversight and prudential supervision by the Bank

The Bank has responsibilities in both oversight and prudential supervision of FMIs, custodians, PSPs, such as PIs and ELMIs, and critical service providers. Oversight and prudential supervision of FMIs differ in a number of areas, ranging from the object of the function, the authority being responsible, the topics covered, as well as the regulatory framework and tools used. However, both oversight and prudential supervision activities, and the framework they are relying on, evolve over time.

Central banks have always had a close interest in the safety and efficiency of payment, clearing and settlement systems. One of the principal functions of central banks is to be the guardian of public confidence in money, and this confidence depends crucially on the ability of economic agents to transmit money and financial instruments smoothly and securely through payment, clearing and settlement systems. These systems must therefore be strong and reliable, available even when the markets around them are in crisis and never themselves be the source of such crisis. FMI oversight pursues these objectives by monitoring systems, assessing them and, where necessary, inducing change. It is now generally recognised as a core responsibility of central banks.

The Bank's oversight of payment, clearing and settlement infrastructures is based on Article 8 of its organic law[1] and focuses on systems established in, or relevant for Belgium. Although SWIFT is neither a payment, clearing or settlement infrastructure, many of such systems use SWIFT which makes the latter a critical service provider of systemic importance. SWIFT is therefore subject to a (cooperative) central bank oversight arrangement.

The Bank is also micro-prudential supervisory authority for individual financial institutions[2], including the operators of clearing and settlement systems, such as CCPs and CSDs, as well as custodians and PSPs like PIs and ELMIs. As of November 2014, a substantial part of the Bank's prudential responsibilities for credit institutions were transferred to the ECB under the single supervisory mechanism (SSM) Regulation[3]. Significant institutions, such as Bank of New York Mellon SA/NV (BNYM SA/NV), are directly supervised by the SSM. However, less significant institutions remain under the prudential supervision of the Bank as national competent authority.

Some FMIs are subject to both oversight and prudential supervision, typically if an FMI is operated by a bank (as is the case for Euroclear Bank). The oversight activity and prudential supervision are, in such situations, complementary in nature: while the oversight activity focuses on the sound functioning of the settlement system (by assessing compliance with oversight standards such as the 2012 CPMI-IOSCO Principles for FMIs (PFMIs)), the prudential supervision focusses on the financial soundness of the operator (by assessing compliance with banking regulations). As a result, oversight and

(1) Article 8, Law of 22 February 1998 establishing the Organic Statute of the National Bank of Belgium, *Belgian Official Gazette* 28 March 1998, 9.377.

(2) The foundations of the 'twin peaks' model were laid by the Law of 2 July 2010 amending the Law of 2 August 2002 on the supervision of the financial sector and financial services, and the Law of 22 February 1998 establishing the Organic Statute of the National Bank of Belgium, and containing miscellaneous provisions, Belgian Official Gazette, 28 September 2010, 59.140. See in particular Article 26, § 1, of the said Law. The new supervision model was established by the promulgation of the Royal Decree of 3 March 2011 on the evolution of the supervisory architecture of the financial sector, *Belgian Official Gazette* 9 March 2011, 15.623. This Royal Decree entered into force on 1 April 2011.

(3) Regulation (EU) No. 1024/2013 of the Council of 15 October 2013 conferring specific tasks on the European Central Bank concerning policies relating to the prudential supervision of credit institutions, *OJ*. 29 October 2013, L. 287, 63–89 (http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013R1024&from=en).

prudential supervision, typically cover different topics. One of the main priorities of oversight relates to the prohibition and containment of any transmission of financial or operational risks through an FMI or critical service provider. Typical areas oversight is focussing on cover the functioning of the system and how its organisation and functioning minimises or avoids risks for itself but – just as importantly – for its participants. Examples thereof include settlement finality rules reducing risks linked to the insolvency of participants (which prevent automatic unwinding of other participants' previous transactions with a bankrupt participant), delivery versus payment or payment versus payment mechanisms eliminating principal risks in transactions between participants, fair and open access for participants, and stringent requirements on business continuity plans ensuring continuity of services for participants. Oversight also takes into account risks related to system interdependencies (either via connected systems or participants) that could provoke contagion risks in financial markets. Prudential supervision intends to ensure that institutions are financially robust at micro-prudential level, thus helping to maintain the trust of the institution's counterparties and, in this way, promoting financial stability. For credit and liquidity risk in particular, oversight looks at intraday credit use and liquidity needs, while banking supervision rules are usually targeting end-of-day positions.

As a consequence of such divergences in scope, oversight and prudential supervision are relying on different frameworks. For oversight, the PFMIs cover payment systems, securities settlement systems, CSDs, CCPs and trade repositories. For the implementation of these principles, further clarity is provided by relevant guidelines such as the CPMI-IOSCO guidance on cyber resilience for FMIs or guidance on resilience and recovery of CCPs. In addition, the CPMI has also published an analytical framework for distributed ledger technology in payment, clearing and settlement. If FMIs have banking status, or for other types of institutions such as custodians, prudential supervision is based on applicable banking legislation (Capital Requirements Directive, Bank Recovery and Resolution Directive, etc.).

The tools to conduct oversight and prudential supervision may differ too. Oversight is generally based on principles and guidelines designed in international fora (Eurosystem, CPMI, CPMI-IOSCO). The traditional approach for enforcing them was to urge FMIs and critical service providers to adhering to them via central bank moral suasion (so-called "soft law" approach). Prudential supervision on the other hand, has laid down its requirements in a formal legal framework enacted through EU Directives, Regulations and local laws ("hard law" approach). Relatively recently, however, central bank oversight has become more formal, owing to the expanding role of the private sector in providing payment and settlement systems, as well as the growing criticality of these systems' proper functioning. In a growing number of cases, oversight is evolving into a hard law approach as illustrated, for example, by the fact that the ECB has laid down its expectations in the ECB Regulation on oversight requirements for systemically important payment systems, or by the 2017 Belgian law on systemically relevant processors of payment transactions. Also, the EU transposed the PFMIs for CCPs and CSDs through a Regulation. EMIR[(1)] sets out the clearing obligations and requirements for CCPs whereas CSDR[(2)] introduces prudential requirements for the operation of CSDs, banking-type ancillary services provided by CSDs or designated credit institutions. In both cases, the Bank has been assigned as the competent supervisory authority for Belgian (I)CSDs, and is, as overseer, also considered as relevant authority under CSDR[(3)].

Apart from (I)CSDs and CCPs, another institution that is subject to both prudential supervision and oversight is Worldline SA/NV, respectively due to its role as acquirer and processor of retail payment instruments. In order to pool expertise and reinforce the synergies between the oversight function and that of prudential supervision, these two functions have been integrated into the same department within the Bank to ensure that its prudential supervision and oversight approach are aligned.

Table 1 below provides an overview of the systems and institutions supervised and/or overseen by the Bank. In addition to the type of services provided, they have been further grouped according to: (i) the type of regulatory role of the Bank (i.e. prudential supervisor, overseer or both) and (ii) the system/institution's international dimension (the Bank as solo authority, international cooperative arrangement with the Bank as lead or in another role). For the systems and institutions established in Belgium which are systemically relevant in other jurisdictions' financial markets or for the

(1) Regulation (EU) No. 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories, *OJ*. 27 July 2012, L. 201, 1-59.
(2) Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012, *OJ*. 28 August 2014, L. 257, 1-72.
(3) The FSMA is assigned, together with the Bank, as national competent authority for CCPs under EMIR.

TABLE 1 THE BANK'S OVERSIGHT AND PRUDENTIAL SUPERVISION OF FINANCIAL MARKET INFRASTRUCTURES, CUSTODIANS, PAYMENT SERVICE PROVIDERS AND CRITICAL SERVICE PROVIDERS

	International supervisory college / cooperative oversight arrangement		NBB solo authority
	NBB lead authority	NBB takes part, other authority is lead	
Prudential supervision		Custodian Bank of New York Mellon SA (BNYM SA/NV)	Custodian BNYM Brussels branch
			Payment Service Providers (PSPs) 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 Remittance: Africash, Belmoney Transfert, Gold Commodities Forex, HomeSend, MoneyGram International, Money International, MoneyTrans Payment Services, Travelex* *Direct Debit: EPBF* *Hybrid: BMCE EuroServices, Cofidis, eDebex, FX4BIZ, Oonex, PAY-NXT, Santander CF Benelux* Electronic Money Institutions (ELMIs) *Buy Way Personal Finance, Fimaser, HPME, Imagor, Ingenico Financial Solutions, Ingenico Payment Services, Loyaltek Payment Systems, RES Credit*
Prudential supervision & Oversight	CSD Euroclear Belgium (ESES) ICSD Euroclear Bank SA/NV	CCPs LCH.Clearnet Ltd (UK), ICE Clear Europe (UK) LCH.Clearnet SA (FR), Eurex Clearing AG (DE), EuroCCP (NL), Keler CCP (HU), CC&G (IT)	
	Assimilated settlement institution Euroclear SA/NV (ESA)		Processor for retail payment instruments Worldline SA/NV
Oversight	Critical service provider SWIFT	Critical service provider TARGET2-Securities (T2S)(1)	CSD NBB-SSS
		Payment systems TARGET2 (T2)(1) CLS Bank	Card payment schemes Bancontact(1) MasterCard Europe(1)
			Payment system Centre for Exchange and Clearing (CEC)(1)

Post-trade infrastructures	Securities clearing	Payments	Payment systems
	Securities settlement		Payment institutions & electronic money institutions
	Custody		Processor for retail payment instruments
Critical service providers	TARGET2-Securities		Card payment schemes
	SWIFT		

Source: NBB.
(1) Peer review in Eurosystem/ESCB.

financial industry as a whole, the Bank has established cooperative arrangements with other authorities[1]. This may involve multilateral cooperative arrangements, in which the Bank acts as lead overseer (Euroclear, SWIFT). The Bank also takes part in a number of international cooperative arrangements (CCPs, BNYM SA/NV, TARGET2, TARGET2-Securities and CLS Bank) in which another national authority acts as lead overseer/supervisor. Domestically, the Bank cooperates with the FSMA which has responsibilities in the supervision of financial markets with regard to conduct of business rules. Annex 2 illustrates the organisation structure of FMIs with an international dimension established in Belgium.

(1) In line with CPMI-IOSCO Responsibility E (cooperation between authorities). The Bank intends – through this report – to inform other authorities with whom the Bank does not have a formal cooperation but that may be interested in understanding the applicable framework, the regulatory approach and the main supervisory priorities.

2. Securities clearing, settlement and custody

FMIs and financial institutions that provide securities clearing, settlement and custody services are considered part of the post-trade securities landscape. Systems that clear trades conducted on a stock exchange or concluded between counterparties on the OTC market, as well as the systems that settle the obligations of the buyer and seller of a trade are subject to oversight. The institutions that operate these systems are subject to supervision. Box 1 provides more insight into the different roles institutions play at each stage of the securities trading, clearing, settlement and custody process while chart 2 depicts the scope of the Bank's oversight and supervision role in this area.

Section 2.1 covers CCPs which systemic relevance has grown after new legislation made central clearing for standardised OTC derivatives mandatory. CCPs are subject to both prudential supervision and oversight. While there is no CCP established in Belgium, under the EMIR Regulation, the Bank takes part as a competent authority in seven CCP colleges as the CCP is settling in a Belgian CSD or due to the size of Belgian clearing members' contribution to the mutual CCP default fund which is available to the CCP to cover the default of a clearing member.

(I)CSDs, responsible for the last stage in the post-trade chain, are dealt with in section 2.2. Of the three (I)CSDs that Belgium hosts, only Euroclear Bank has banking status (rated AA+ by Fitch Ratings and AA by Standard & Poor's) and falls under the prudential authority of the ECB. However, as it has been qualified as an LSI under the SSM (i.e. total assets < € 30 billion), it remains under the direct prudential supervision of the Bank.

As the risk profile of an FMI is fundamentally different from a universal deposit-taking bank, prudential requirements for banks (Basel III, Capital Requirements Directive, etc.) do not always adequately cover the specific operational and financial risks involved. Other internationally agreed standards for CCPs and (I)CSDs are more adequate for covering such risks (i.e. PFMIs). In the EU framework, these principles have been transposed into EU legislation (EMIR and CSDR).

(I)CSDs established in Belgium have a different scope in terms of activities. While Euroclear Bank provides services in a wide range of securities, securities eligible in Euroclear Belgium are primarily Belgian equities. Euroclear Bank and Euroclear Belgium are subject to both prudential supervision and oversight. Under the CSDR, the Bank has been assigned as the sole competent supervisory authority for Belgian CSDs, and is, as overseer, also considered as relevant authority in the CSDR.

NBB-SSS holds and settles public sector debt including securities issued by the Belgian federal government and by regional or local governments as well as private sector debt issued by corporates, credit institutions or other entities. NBB-SSS is subject to oversight only.

Euroclear Belgium and NBB-SSS's daily settlement operations are outsourced to TARGET2-Securities (T2S), as in the case of other CSDs in Europe[1]. T2S is not a CSD, but as it provides critical settlement services to many euro area and non-euro area CSDs, it is essential that it enables member CSDs to comply with the regulations applicable to them. In line with PFMI Responsibility E (Cooperation with other authorities), the Eurosystem has set up the T2S Cooperative Arrangement to ensure that all authorities with a legitimate interest in the smooth functioning of T2S are involved, including the overseers and market authorities of CSDs that have signed the T2S Framework Agreement, in coordination with the ECB and ESMA. The authorities assess both the general organisation of T2S as a critical infrastructure (i.e. technical platform, legal basis, governance structure and comprehensive risk management framework), as well as the services it provides against an applicable subset of the PFMIs. The Bank is involved in the cooperative oversight of T2S[2].

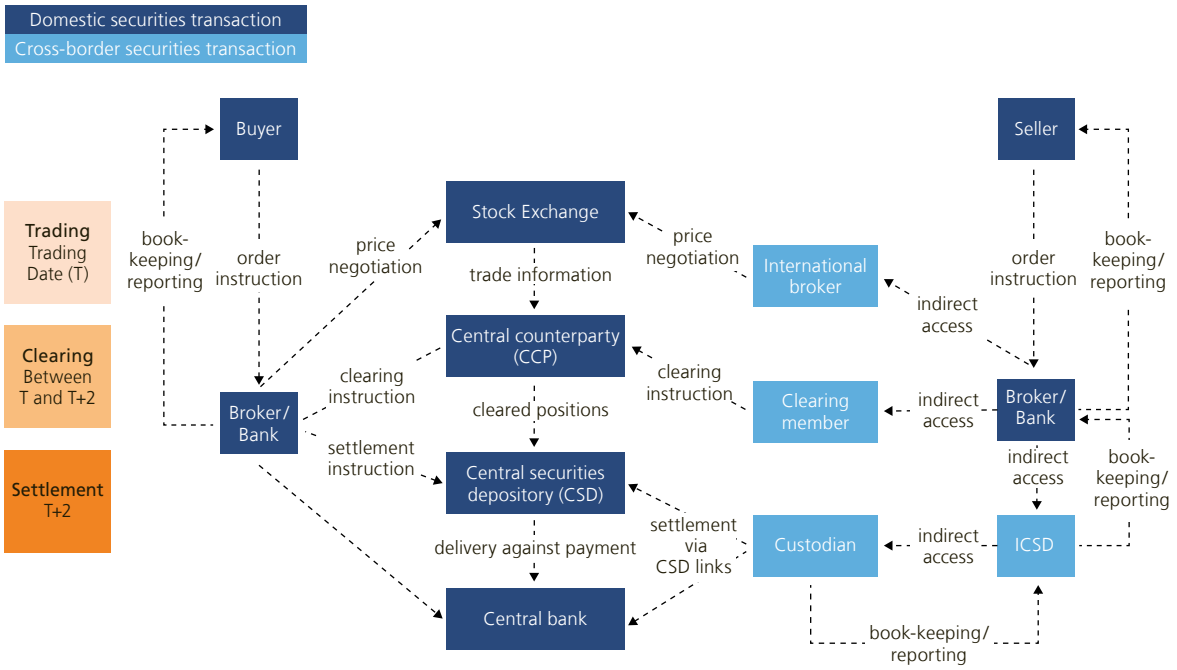
(1) In December 2017, T2S settled on average 571 879 transactions per day for an average daily value of € 884.4 billion (source: ECB).
(2) Oversight activities of the Eurosystem on T2S are covered in the Eurosystem's Oversight Report. The last report was published in November 2017 covering reporting year 2016. See also https://www.ecb.europa.eu/pub/pdf/other/eurosystemoversightreport2016.en.pdf?2ae0c243b5cab226b6d21c0115dbf609.

Box 1 – Institutions' role at each stage of the securities trading, clearing, settlement and custody process

The lifecycle of a securities trade until its settlement typically involves various stages and intermediaries. The chart below provides an example for a domestic and a cross-border transaction. For the domestic transaction, it is assumed that institutions have direct access to securities trading, clearing and settlement infrastructures, while for the cross-border trade, it is assumed institutions have to rely on intermediaries to connect to those infrastructures.

The domestic transaction is concluded on a stock exchange on behalf of the buyer and seller of securities. The buyer and seller will instruct their respective brokers (or banks) to process a buy or sell order on the stock exchange based on their price indication. At this stage (on trade day T), the order is executed in the market by the respective brokers but the buyer does not own the securities yet (i.e. no movement between buyer and seller securities accounts). The brokers have direct access to the CCP that will step in and net trade positions by becoming the seller to the buyer and vice versa. After clearing, instructions to settle the net positions are sent to the CSD. To settle securities against cash on the settlement date (e.g. on T+2), a CSD is typically connected with the payment system of the central bank. The seller's broker will deliver the securities (i.e. net amount after clearing by the CCP) and receive the cash on behalf of its client. The broker of the buyer will process the other way around. This stage marks the transfer of ownership from the seller to the buyer as it implies an effective movement between securities accounts.

For the cross-border transaction, the seller's broker (or bank) can rely on an international broker to conclude the transactions on the stock exchange. Because of the cross-border nature of the transaction, counterparties may not be directly connected to the CCP and may therefore opt to use a clearing member of the CCP. Clearing members have to provide collateral (margin) to cover the risks for the CCP. Brokers may also use an ICSD for holding foreign securities. In turn, an ICSD may use a custodian to connect to the local CSD and central bank. The local custodian (or ICSD) will ensure book-keeping and reporting services on the holding of securities, as well as other custody services such as the processing of dividend payments.

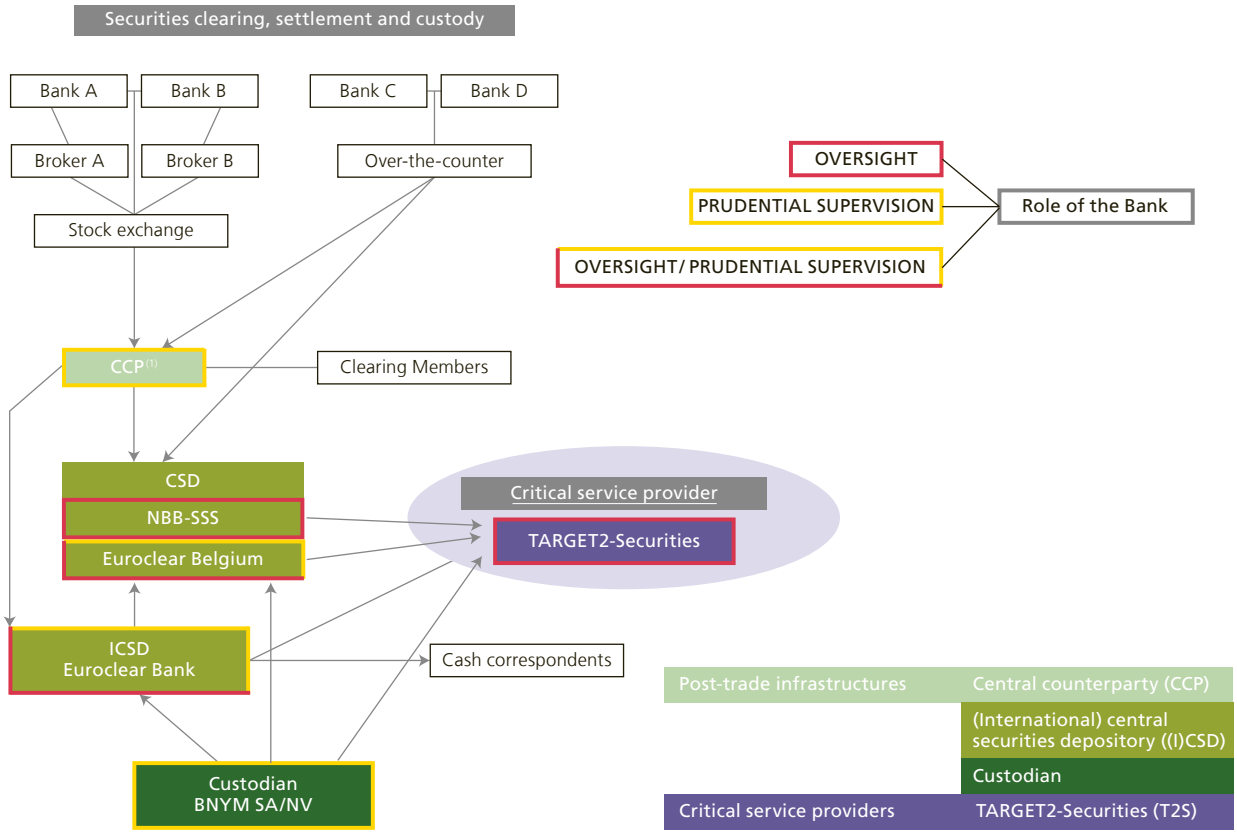


– Trading (no movements on securities accounts on behalf of buyer and seller).
– Clearing (calculation of net positions, no movements on securities accounts).
– Settlement (exchange of cash and securities, movements on securities accounts on behalf of buyer and seller).

Source: NBB.

Finally, section 2.3 covers institutions whose single business line is the provision of custody services (i.e. providing securities safekeeping, settlement and investor services to their clients) with a focus on BNYM SA/NV which is a global custodian established in Belgium with links to multiple (I)CSDs allowing its clients to hold securities issued in markets worldwide.

CHART 2 SCOPE OF THE BANK'S OVERSIGHT AND PRUDENTIAL SUPERVISION ROLE IN THE POST-TRADE SECURITIES LANDSCAPE



Source: NBB.
(1) LCH.Clearnet Ltd (UK), ICE Clear Europe (UK), LCH.Clearnet SA (FR), Eurex Clearing AG (DE), EuroCCP (NL), Keler CCP (HU), CC&G (IT).

2.1 CCPs

Changes in regulatory framework

With the introduction of the clearing obligation – this is, the mandatory use of a CCP – for standardised OTC derivatives contracts, CCPs have become increasingly critical components of the financial system. Back in 2015, the Financial Stability Board (FSB) had set out a workplan to strengthen CCP resilience, and ultimately, its resolvability if need be[1].

In mid-2017, the FSB published its guidance on CCP Resolution and Resolution Planning[2]. The guidance complements the FSB Key Attributes of Effective Resolution Regimes in the case of CCPs. It sets out powers for resolution authorities to maintain the continuity of critical CCP functions; discusses the use of loss allocation tools; and describes steps authorities should take to establish crisis management groups for relevant CCPs and to develop resolution plans. Items covered include the timing of entry into resolution; the adequacy of financial resources; the tools for returning to a matched book and for allocating default and non-default losses, the application of the no-creditor-worse-off safeguard in the event of resolution[3], and the cross-border cooperation and effectiveness of resolution actions.

(1) Available at: http://www.fsb.org/2015/09/2015-ccp-workplan/.
(2) Available at http://www.fsb.org/2017/07/guidance-on-central-counterparty-resolution-and-resolution-planning-2/
(3) CCP participants, equity holders and creditors should have a right to compensation if they do not receive in resolution a minimum of what they would have received, had the CCP or relevant clearing service been liquidated or terminated under the applicable insolvency law instead.

Under the FSB's guidance, the BCBS, CPMI and IOSCO completed their main policy work to enhance the resilience, recovery planning and resolvability of CCPs, focusing on CCPs that are systemic across multiple jurisdictions.

In early July 2017, the BCBS, CPMI, FSB and IOSCO also published their first joint Analysis of Central Clearing Interdependencies[1], covering 26 CCPs from 15 jurisdictions and analysing the interdependencies between CCPs and their clearing members and other financial services providers, such as liquidity providers. The analysis shows a core of highly connected CCPs and financial institutions.

In July 2017, CPMI-IOSCO issued a final report on the Resilience of CCPs[2] that contains guidance to the PFMIs, in an effort to further improve the CCPs' resilience. It covers aspects of the CCP's governance, credit and liquidity stress-testing, margining, a CCP's contribution of its financial resources to losses, and what constitutes adequate coverage of the CCP's credit and liquidity resource requirements.

At the same time, the CPMI and IOSCO updated their report on the recovery of FMIs[3] with proposed additional guidance providing more granularity to the PFMI standards. The changes are limited in scope and relate to the following four areas: i) the effective organisation of the recovery plan; ii) the arrangements (timing) for replenishing the CCP default fund after a clearing member default; iii) the recovery by the CCP of losses not related to the default of a clearing member, such as custody and investment risks; and iv) transparency with respect to the recovery tools and their implementation.

In April 2018, CPMI and IOSCO published a framework for supervisory stress testing of CCPs[4] with a view to analysing the broad, macro-level impact of a common stress event affecting a set of CCPs. The sources of stress can be credit or liquidity occurrences, or both. The stress-testing framework is broadly designed and flexible and its addressees are the authorities, and not the CCPs, and its use is voluntary. In Europe, ESMA already stress tests EU CCPs on such a basis (see hereafter, item "Prudential & oversight approach").

In the EU, EMIR and its implementing Regulations set out the clearing and reporting obligation for standardised derivatives[5], the requirements for CCPs established in the EU and their supervision. In May 2017, the European Commission tabled a proposal to amend EMIR, the so-called EMIR Refit proposal. It aims to eliminate disproportionate costs and burdens to small companies – especially non-financial counterparties notably by simplifying some requirements relating to the reporting and the clearing obligation. Overall, the main focus is on fine-tuning requirements or increasing the efficiency.

In mid-2017, the Commission also proposed to improve consistency of supervisory arrangements for CCPs established in the EU, and to enhance the EU's ability to monitor, identify and mitigate third-country CCP risks[6]. ESMA governance would effectively be enhanced, while central banks responsible for EU currencies would be given a bigger role. Issuing central banks would be in charge of the CCP's payment and settlement arrangements, and liquidity risk management. This aspect is complemented by an ECB proposal to obtain regulatory powers vis-à-vis CCPs in the context of its monetary policy[7]. Furthermore, the Commission's proposal sets out a direct supervision regime for systemic third-country CCPs, and even makes it possible to require – via a delegated act – the relocation to the EU of so-called "substantially systemically important CCPs". In this respect, it prepares for a March 2019 Brexit, by strengthening the third-country CCP authorisation and supervisory regime. Discussions in the EU Council of Ministers and European Parliament are still ongoing.

A more detailed proposal from the Commission that sets out the CCP recovery and resolution frameworks, based on international work, is still being discussed by the EU Council and European Parliament. It will create a framework to ensure the continuity of a CCP's critical functions while avoiding the use of taxpayers' money to restructure and resolve the CCP. The national resolution authority would be able to sell parts of the CCP business to a third party,

(1) Available at http://www.fsb.org/2017/07/analysis-of-central-clearing-interdependencies/
(2) Available at https://www.bis.org/cpmi/publ/d163.htm
(3) Available at https://www.bis.org/cpmi/publ/d162.htm.
(4) Available at https://www.bis.org/cpmi/publ/d176.htm.
(5) The clearing obligation has been in force since mid-2016, for standardised interest rate swap contracts in the most relevant currencies, and for index-linked credit default swaps. ESMA holds a "Public register for the clearing obligation under EMIR" available on its website at https://www.esma.europa.eu/regulation/post-trading/otc-derivatives-and-clearing-obligation.
(6) The Commission's legislative proposal is available at http://europa.eu/rapid/press-release_IP-17-1568_en.htm.
(7) The ECB proposal of June 2017 to adapt the Art. 22 of the ECB Statutes to that end is available at http://europa.eu/rapid/press-release_IP-17-1568_en.htm.

eventually a bridge CCP and to terminate contracts and allocate losses via haircutting variation margins and/or applying a resolution cash call. The Bank's point of view is that there must be a harmonious division of responsibilities and tasks; i.e. the allocation to EU and national authorities of fiscal responsibility for CCP resolution should mirror the division of tasks of CCP supervision.

Prudential and oversight approach

From a microprudential perspective, the most relevant financial risks faced by a CCP are counterparty risk and liquidity risk. Counterparty credit risk refers to the risk that a counterparty will be unable to fully meet its obligations, mainly if a clearing member defaults in extreme markets. Liquidity risk will chiefly arise when the CCP seeks to re-establish a balanced book under these conditions. To cope with these risks (according to EMIR), a CCP must at all times be able to withstand the simultaneous default of its two biggest clearing members in extreme but plausible markets, and have adequate resources to cover the losses or raise in time the liquidity needed.

In February 2018, ESMA published the results of its second supervisory stress test for EU CCPs. The test focused on both the counterparty credit risks and the liquidity risks which CCPs would face as a result of multiple clearing member defaults and simultaneous market price shocks. The results show CCPs' resilience in extreme but plausible markets, as their resources were sufficient to cover losses resulting from the default of the top two clearing member groups under both historical and hypothetical market stress scenarios. Nor did ESMA detect any major systemic risk concerns for the liquidity stress test part. The report highlights some individual CCP-specific results for the credit stress test; a possible follow-up is one by the competent national authority. Also, more severe stress scenarios than the top two clearing member defaults were applied, and the report contains info on the degree of the interconnectedness of the clearing activities[1].

There is currently no CCP established in Belgium. However, CCPs are relevant for Belgian markets, clearing members and CSDs. These include Eurex Clearing AG in Frankfurt, LCH.Clearnet Ltd in London – which clears interest rate swaps including in euro – and LCH.Clearnet SA in Paris which clears the Euronext Brussels markets. All three CCPs clear repos. For volume and risk data on these CCPs, see Annex 3. Further, the London-based CCP ICEClear Europe is the main EU CCP clearing credit default swaps. As of end 2017, the Bank participated in seven EU CCP supervisory colleges, as listed in table 2, based either on its capacity of supervisor of a CSD that the CCP settles in, or as supervisor of clearing members of the CCP that contribute – on a country-by-country basis – most to the default fund. Box 2 provides an indication how much risk these CCP manage, based on the overall initial margin amounts they receive and their default fund resources.

Supervisory priorities in 2018

Priorities for the ongoing supervision of EU CCPs are set by the national competent authority, taking into account the college members' demands.

In anticipation of EU legislation on CCP resolution, and given the new FSB and CPMI-IOSCO guidance, national competent authorities continue to establish cross-border crisis management groups for CCP resolution and consider how to plan CCP resolution. In turn, CCPs are enhancing their own recovery rules and the way stakeholders, including clearing members, would share in the losses. Another continuing priority remains the CCP's operational – and specifically its cyber risk – management.

In early February 2018, ESMA issued guidance reports on a CCP's conflicts of interest management[2] and started a consultation in January on guidance for anti-procyclicality margin measures for CCPs[3]. National competent authorities are – or will be – expected to follow up their implementation.

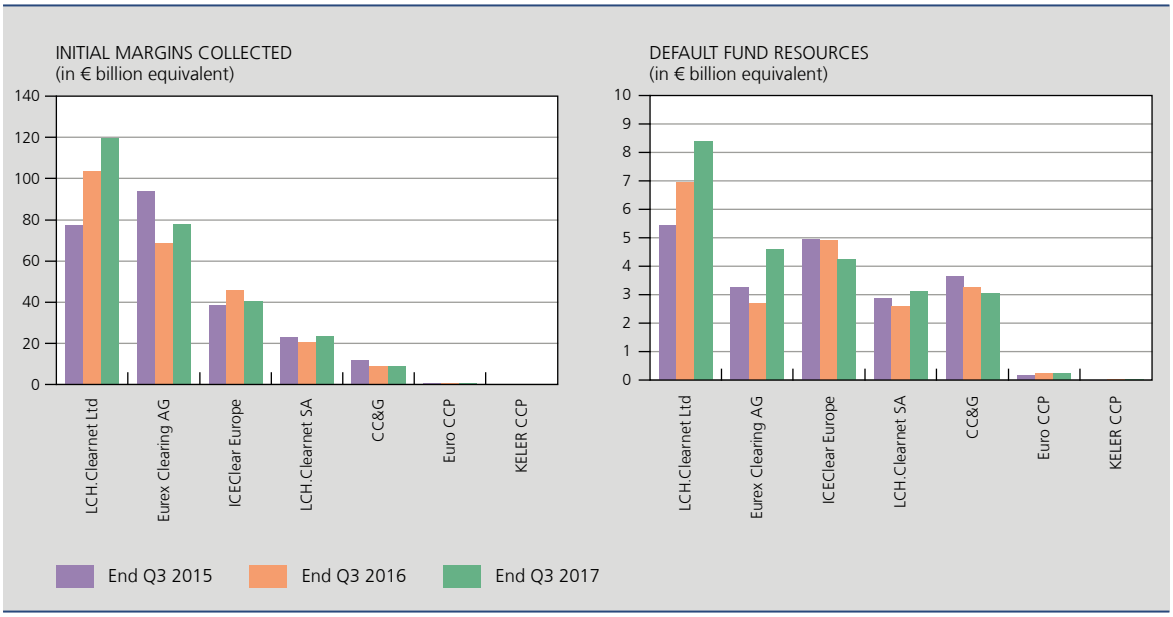
(1) The ESMA report on the second EU wide CCP stress test (2017) can be found at https://www.esma.europa.eu/press-news/esma-news/esma-publishes-results-second-eu-wide-ccp-stress-test.
(2) Available at https://www.esma.europa.eu/press-news/esma-news/esma-issues-conflict-interest-guidelines-ccpsand.
(3) Available at https://www.esma.europa.eu/press-news/esma-news/esma-consults-ccp-anti-procyclicality-margin-measures.

Finally, work is continuing on authorisation of new services or risk models proposed by the CCP. New services or products or significant risk model changes implemented by an EU CCP have to be approved by its national competent authority, which in turn has to take into account the CCP's supervisory college's opinion.

Box 2 – Measuring how much risk a CCP manages

Different indicators can be used to measure the size of CCPs. According to the ESRB[1], applying indicators such as the number of clearing members (including underlying clients), the volumes of transactions processed by a CCP and the value of pre-funded financial resources (i.e. initial margins[2] and the default fund[3]) should not be considered separately. Even if applied in combination, the type of products cleared (and their risk profile), as well as the specific risk management methods used by the CCPs, are relevant to rank a CCP in accordance with its importance.

INITIAL MARGINS COLLECTED AND DEFAULT FUND RESOURCES AVAILABLE TO SELECTED EU CCPS



Sources: CCP websites, NBB calculations.

In addition, evolutions in both the amounts of initial margins and the default fund resources have several drivers. Relevant parameters include the market or product cleared, the activity of the CCP (increase or reduction in cleared volumes affecting the initial margins collected), the volatility of the market or product the CCP (mainly) clears (volatility in derivatives versus repo market segments), the duration of the contracts cleared by the CCP (more initial margins for long-term contracts) or potential diverging implementation of the regulatory requirements of EMIR. However, as the overall structure and requirements for initial margin and default fund calculations are prescribed by the EMIR Regulation, and assuming such rules are consistently applied to CCPs in the EU, initial margin amounts

(1) ESRB, Indicators for the monitoring of central counterparties in the EU, Occasional Paper Series N° 14, March 2018.

(2) Initial margin is collateral that clearing members provide to CCPs to open or maintain a position, covering potential future price movements of a contract or portfolio over the liquidation period in normal markets. The liquidation period is the time needed to sell or hedge a contract or position, e.g. standardly two days for on-exchange contracts.

(3) Clearing members mutualise each other via the CCP's default fund. This pre-funded resource can be used only by the CCP after the initial margin amount of the defaulting clearing member is used to cover the CCP's counterparty credit risk exposure.

received by a CCP across all its clearing members could provide a measure of how much *risk* a CCP manages. The charts below show for those CCPs where the Bank participates in a supervisory college the initial margins collected by the CCPs (left-hand side) and the default fund resources (right-hand side). Based on the above assumption, such data are to a certain extent comparable across CCPs. The data show as well that the ranking of CCPs is not the same from both perspectives. Besides these factors, the level of concentration among clearing members in a particular CCP also has an impact on the size of the default fund to cover the scenario of a simultaneous default of the two largest clearing members.

TABLE 2 EU CCP SUPERVISORY COLLEGES WITH THE BANK'S PARTICIPATION

CCP[1]	Main clearing services and relevance for Belgium	Direct Belgian clearing members[2]	EMIR criterium for the Bank's participation in the CCP's supervisory college	
			Contribution of Belgian clearing members to the CCP default fund	CCP settles in a Belgian (I)CSD[3]
LCH Clearnet Ltd (UK)	Interest Rate Swaps / Repos	4 – AXA Bank Europe, – Belfius Bank; – BNP Paribas Fortis; – KBC Bank		X (EB, NBB-SSS)
Eurex Clearing AG (DE)	Listed interest derivatives / Repos	3 – Belfius Bank; – BNP Paribas Fortis; – KBC Bank		X (EB)
LCH Clearnet SA (FR)	Euronext cash and derivatives trades (including Euronext Brussels)	6 – Banque Degroof Petercam; – Belfius Bank; – BNP Paribas Fortis; – Delen Private Bank; – Leleux Associated Brokers; – Van De Put & Co Private Banks		X (EB, EBE, NBB-SSS)
ICE Clear Europe (UK)	Credit default swaps	none		X (EB)
CC&G (IT)	National CCP of Italy	none		X (EB)
Euro CCP (NL)	Main European stocks	none		X (EB)
Keler CCP (HU)	National CCP of Hungary	1 – KBC Securities Hungarian branch	X	

Source: NBB.

(1) Until November 2016, the Bank was part of the national Polish KDPW_CCP college, but is no longer. Under European rules, CCP college participation is reassessed annually on the basis of EMIR Article 18 criteria.

(2) A Belgian bank not mentioned in the table may clear in a CCP but as an indirect clearing member, this is, as the client of a clearing member that could be a foreign entity of the group it belongs to.

(3) EB: Euroclear Bank ICSD, EBE: Euroclear Belgium CSD, NBB-SSS.

2.2 (I)CSDs

Changes in regulatory framework

Relevant policy-setting bodies are providing additional guidance to the 2012 PFMIs and the 2014 CSDR which regulatory technical standards have become effective as from end-March 2017 [1]. They aim for a consistent and uniform implementation for these sets of principles and rules across jurisdictions.

CPMI-IOSCO published in July 2017 a revised version of its 2014 Recovery Report by providing further guidance on recovery arrangements for FMIs, in particular with regard to (i) operationalisation of the recovery plan; (ii) replenishment of the FMI's financial resources; (iii) non-default related losses; and (iv) transparency with respect to recovery tools and how they would be applied [2].

For CSDR, ESMA published a set of guidelines in March 2017 on CSDs' access to CCPs or trading venues' transaction feeds, specifying the criteria for the comprehensive risk assessment to be conducted by a CCP or trading venue to whom a CSD requested access for their trading feeds [3], as well as guidelines for participant default rules and procedures dealing with how a participant's default should be acknowledged, which actions a CSD may take in such a case, how the CSD should communicate and how it should test and review its default rules and procedures [4].

ESMA has also provided guidance on how cooperation arrangements should be implemented for CSDs providing cross-border services, as this is of growing relevance for the functioning of the securities markets and the protection of investors in the host Member State. Given the need to use consistent data aggregated at EU level for the calculation of the respective indicators, ESMA has decided to issue guidelines on the process for the collection, processing and aggregation of the data and information necessary for the calculation of the indicators to determine (i) the most relevant currencies in which settlement takes place [5] and (2) the substantial importance of a CSD for a host Member State [6]. The guidelines clarify the scope of the data to be reported by CSDs for the purpose of the calculation of different indicators. These indicators are important to identify the relevant authorities under the CSDR framework, in particular for Euroclear Bank given the international dimension of its activities'.

ESMA continues to update its Questions and Answers section regarding the implementation of the CSDR promoting common supervisory approaches and practices in the application of the CSDR [7].

Rules targeting (I)CSDs' participants should be mentioned as well. In March 2017, ESMA published the final draft technical standards on the 2015 Securities Financing Transaction Regulation [8] which aims to increase the transparency of securities financing transactions and requires both financial and non-financial market participants to report details of such transactions to a trade repository.

Prudential and oversight approach

The three (I)CSDs established in Belgium have distinct status, scope and risk profile. The Bank's prudential and oversight approach takes these different dimensions into account. The owner of Euroclear Bank, Euroclear SA/NV, provides core services to its group (I)CSDs, including Euroclear Bank and Euroclear Belgium (see also the Euroclear Group structure in Annex 2). In order to bring Euroclear SA/NV within the Bank's supervisory scope, it has been designated as an "assimilated settlement institution" [9]. The specific international and multicurrency dimension of Euroclear Bank is covered in box 3.

(1) Except for the regulatory technical standards relating to settlement discipline.
(2) Available at: https://www.bis.org/cpmi/publ/d162.pdf.
(3) Available at: https://www.esma.europa.eu/sites/default/files/library/esma70-708036281-7_final_report_on_csdr_guidelines_on_access_0.pdf
(4) Available at: https://www.esma.europa.eu/sites/default/files/library/esma70-708036281-8_final_report_on_csdr_guidelines_on_participant_default_rules.pdf.
(5) Available at: https://www.esma.europa.eu/sites/default/files/library/esma70-708036281-66_csdr_guidelines_on_relevant_currencies_0.pdf.
(6) Available at: https://www.esma.europa.eu/sites/default/files/library/esma70-708036281-67_csdr_guidelines_on_substantial_importance_of_a_csd_0.pdf.
(7) Available at: https://www.esma.europa.eu/press-news/esma-news/esma-updates-its-csdr-qas-0.
(8) Regulation (EU) 2015/2365 of the European Parliament and of the Council of 25 November 2015 on transparency of securities financing transactions and of reuse and amending Regulation (EU) No. 648/2012.
(9) Article 23 of the Law of 2 August 2002 on the supervision of the financial sector and financial services and Art. 10, § 7, of the Royal Decree of 26 September 2005 on the legal status of settlement institutions and assimilated institutions.

CSDR covers prudential requirements for the operation of (I)CSDs, as well as specific prudential requirements for them and designated credit institutions offering banking-type ancillary services. Depending on the scope of services provided, (I)CSDs will have to obtain an authorisation to provide (I)CSD services or both (I)CSD and banking-type ancillary services. For the latter, an (I)CSD will be authorised to offer such services by itself [1] or to designate one or more credit institutions for that purpose. If two (I)CSDs are linked to each other through mutual operational procedures, any such interoperable link needs to be licensed as well. Under the CSDR, the Bank is the competent (as supervisor) and relevant (as overseer) authority for the CSDs established in Belgium. The Bank seeks the FSMA's advice for aspects that fall under the latter's perimeter of competence for CSDs as part of its tasks of ensuring compliance with rules guaranteeing the sound operation, integrity and transparency of financial instruments markets, as well as its work on ensuring compliance with the rules for protecting the interests of investors in financial instrument transactions [2]. A protocol setting out the cooperation arrangements has been concluded.

Euroclear Belgium and Euroclear Bank need to be "re-authorised" as a CSD. Euroclear Bank has to file not only for a CSD licence but also for a banking licence and for the interoperable link with Clearstream Banking Luxembourg. For NBB-SSS, which is operated by the Bank, the rules for authorisation and supervision of (I)CSDs under the CSDR are not applicable; i.e. members of the ESCB, Member States' national bodies performing similar functions or other public bodies do not need to be authorised under the CSDR [3]. However, from a legal perspective, NBB-SSS needs to be compliant with the CSDR no later than one year after the March 2017 entry into force of the CSDR regulatory technical standards. NBB-SSS was assessed to comply with the CSDR requirements at the end of March 2018.

For Euroclear Belgium and Euroclear Bank, the Bank received the CSDR application files at the end of September 2017. The application was considered incomplete due to the absence of information required under CSDR, ongoing IT developments which needed to be completed for CSDR compliance and the pending implementation of new policies and procedures in line with CSDR. The Bank has set deadlines for Euroclear Belgium and Euroclear Bank to provide additional information (see section on supervisory priorities in 2018). This conclusion was based on the pre-assessment conducted by the Bank in the course of 2017. For Euroclear Belgium, this pre-assessment was coordinated with the Dutch and French authorities as Euroclear Belgium shares a common rule book with Euroclear France and Euroclear Nederland (Euroclear Settlement of Euronext-zone Securities or ESES for short).

Still in the case of Euroclear Bank, and in addition to the CSDR pre-assessment, the Bank did further work on the update of the PFMI assessment, and in particular on the Principles related to banking-type ancillary services (i.e. Principle 4, 5 and 7 on respectively credit risk, collateral and liquidity risk). Credit use by participants in the system, which is secured and, as a rule, intraday, is the main source of Euroclear Bank's liquidity needs. As Euroclear Bank provides settlement services in multiple currencies, liquidity risks should be considered per currency. Euroclear Bank has enhanced its risk management framework by implementing a multicurrency *ex-ante* control framework (i.e. limits are set by currency depending on its qualifying liquid resources in that currency), as opposed to an *ex-post* control framework (i.e. whereby measures are taken by the (I)CSD afterwards based on the outcome of back-test liquidity stress scenarios). In that context, Euroclear Bank has strengthened its access to liquidity in multiple currencies, including by extending its committed facilities. At the same time, the type of qualifying liquid resources it relies on has been reviewed. For the PFMI assessment, the Bank consults and considers the views of the other authorities of the Multilateral Oversight Group (i.e. Federal Reserve, Bank of England, Bank of Japan, ECB as observer – see table 3 below).

The Bank also monitored the review of risk governance in Euroclear Bank [4] and in particular the roles of the three lines of defense (i.e. operations department as 1st line managing risks on a day-to-day basis, risk management as 2nd line assisting in determining risk capacity and risk appetite and monitoring/reporting material risks and internal audit as 3rd line providing an independent review on the overall effectiveness of the risk governance framework). Specific attention is given to the capability of the 1st line to define potential risk events and their corresponding risk

(1) In the EU, only five (I)CSDs are currently licensed as a bank, namely Euroclear Bank (BE), Clearstream Banking Luxembourg (LU), Clearstream Banking Frankfurt (DE), Keler (HU) and OeKB (AT).

(2) The rules on conflicts of interest, record-keeping, the requirements concerning participation, transparency, procedures for communicating with participants and other market infrastructures, the protection of the assets of participants and their clients, freedom to issue securities via any CSD authorised in the EU, and access between a CSD and another market infrastructure.

(3) Article 1.4., Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No. 236/2012, OJ. 28 August 2014, L. 257, 1-72.

(4) Workstream based on a self-assessment of Euroclear Bank against a set of international and European principles and guidelines on strengthening risk management practices which should be implemented by financial institutions as part of the ICAAP.

responses. Risk management as 2nd line is in charge of challenging these risk responses within the boundaries set by the risk appetite framework. As a prudential supervisor, the Bank reviews adherence of existing practices of Euroclear risk management to these principles and guidelines as part of the SREP[1] which may trigger additional capital requirements if deemed necessary by the Bank. Essential components, such as Euroclear's risk appetite framework and internal control system, are being updated under the CSDR. This review on risk governance is ongoing and will be continued in 2018.

Further work was also done on the recovery plans for Euroclear Group entities subject to the Bank's supervision and oversight; i.e. Euroclear SA/NV, ESES/Euroclear Belgium and Euroclear Bank. The Bank makes use of the specific guidelines on recovery plans that are applicable to Belgian credit institutions and Belgian parent undertakings of credit institutions which have the regulatory status of CSD or assimilated settlement institution, as well as for Belgian CSDs which do not have the regulatory status of credit institution[2]. In this process, the Bank considers views and comments from other regulators, i.e. relevant Euroclear Group authorities for the recovery plans for Euroclear SA/NV and ESES/Euroclear Belgium and the Multilateral Oversight Group for the Euroclear Bank recovery plan. Further work will be conducted on scenarios of unexpected credit losses and liquidity shortfalls that could be encountered in extreme, but plausible scenarios.

In accordance with applicable supervisory rules[3], the Bank assessed several institutional developments with regard to the Euroclear Group. At the end of November 2017, Euroclear Bank established a branch in Japan after approval by the Bank and Japan's Financial Services Agency. At group level, some changes occurred in the shareholdership. Intercontinental Exchange (ICE), owner of several exchanges for financial and commodity markets including NYSE, acquired 10 % of the shares of the Euroclear plc, the ultimate holding company of the Euroclear group. This acquisition was done in two stages, the first at the end of October 2017 with 4.7 % of total shares, while the second stage was subject to the Bank's approval[4] as ICE's stake in Euroclear plc increased from 4.7 % to 10 %.

Within the broader framework of a strategic review of NBB-SSS activities and after successful integration into T2S (March 2016), the Bank assessed in the course of 2017 the potential (dis)continuation of NBB-SSS. Its user committee and other stakeholders such as Febelfin, the Belgian Federal Public Service Finance and the ECB were all consulted. In October 2017, the Bank decided to keep NBB-SSS going in the future[5]. The Bank's oversight team followed up on the measures taken by NBB-SSS to allow settlement against payment in GBP (via the Bank's cash account with the Bank of England) and DKK (via participants' cash accounts with the Danish central bank).

Another priority for Belgian (I)CSDs continues to be cyber resilience. The Bank has reviewed the respective self-assessments against the June 2016 CPMI-IOSCO guidance on cyber resilience for FMIs that provide additional guidance to the PFMIs on how FMIs can enhance their cyber resilience capabilities to limit the growing risks that cyber threats pose for them, and thus for financial stability in general. In the same domain, further work is being conducted with regard to end-points of payment and securities settlement systems in the framework of cyber heists targeting the high-value transaction chain (see chapter 4 on SWIFT and the article on endpoint security strategies). As Euroclear SA/NV provides IT services to the Euroclear Group (I)CSDs, this workstream is coordinated through a Cyber Security Task Force encompassing regulators of all group entities which is chaired by the Bank.

(1) Supervisory Review and Evaluation Process.

(2) Recognised by Article 12, Royal Decree of 26 September 2005 concerning the status of settlement institutions and assimilated settlement institutions, *Belgian Official Gazette* 11 October 2005, 43.507. This circular covers the requirements of both BRRD and CPMI-IOSCO in that respect.

(3) For purposes of prudential supervision, Euroclear Bank and Euroclear SA/NV have been designated as a "Systemically important financial institution" (SIFI) and are therefore subject to supervisory rules under the law of 22 February 1998. This means in particular that the Bank has a right of non-objection to strategic decisions should they create a material risk for the stability of the financial sector and may impose specific measures in that regard.

(4) Based on the Banking law and Royal Decree of 26 September 2005.

(5) Available at: https://www.nbb.be/doc/ti/nbbsss_strategic_reflection_decision.pdf.

Box 3 – International dimension of Euroclear Bank

By the very nature of its business model, Euroclear Bank is internationally oriented. This international dimension of Euroclear Bank is reflected in several areas like participants, currencies and linked securities markets. At the end of 2017, Euroclear Bank counted about 1 600 participants located in more than 90 countries. Its participant base consists mainly of non-domestic participants, including more than 100 central banks, about 15 CCPs and CSDs, as well as credit institutions, broker-dealers and investment banks.

Apart from its notary function for international bonds, notably Eurobonds, which it mainly shares with Clearstream Banking Luxembourg, Euroclear Bank aims to provide its participants with a single gateway to access many foreign securities markets (i.e. Euroclear Bank has a link with foreign CSDs which act as notary for securities issued in the local market). When (I)CSDs offer their participants access to foreign securities markets, they are considered as "investor (I)CSDs", whereas the foreign (I)CSDs are referred to as "issuer (I)CSDs". As of 2018, Euroclear Bank is connected to more than 50 foreign CSDs as "investor ICSD" in domestic markets.

To provide services in international bonds and a wide range of foreign securities, about 100 different currencies are eligible in the system operated by Euroclear Bank; i.e. 51 settlement currencies[(1)] and 49 denomination currencies[(2)]. Securities can be settled against payment in a Euroclear settlement currency which can be different from the denomination currency. Denomination currencies are used as units of account for securities balances but not for payment transactions.

At the end of 2017, the value of securities deposits held on Euroclear Bank's books on behalf of its participants amounted to € 12.8 trillion equivalent (up from € 12.7 trillion in 2016). After EUR (49 %), USD is the main denomination currency (28 %), followed by GBP (11 %). 53 % of securities deposits are in international bonds, such as Eurobonds, for which issuers can choose the currency or country of issue.

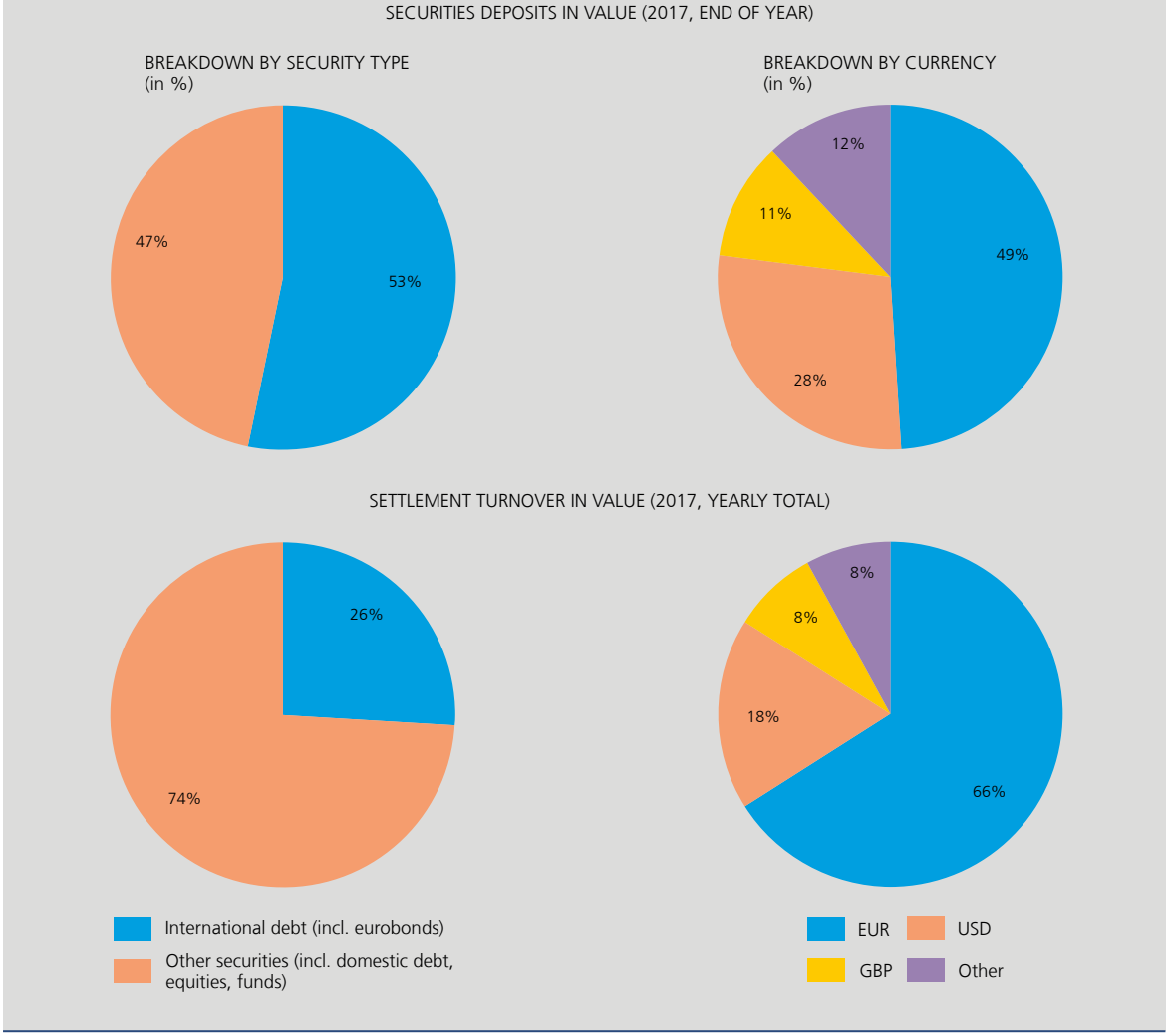
Regarding settlement turnover, the number of transactions settled in 2017 in Euroclear Bank amounted to 95.4 million (up from 84.1 million in 2016). In value terms, this represents € 498.1 trillion (up from € 451.7 trillion in 2016). On average, Euroclear Bank processes more than 360 000 transactions daily with a total value of € 1.9 trillion. 66 % of settlement turnover, free of payment and against payment transactions, was denominated in EUR, after USD (18 %) and GBP (8 %). In terms of settlement turnover per security type, compared to securities deposits, international debt accounts for 26 % while the bulk is composed of other types of securities such as domestic debt and, to a lesser extent, equities or exchange-traded funds.

The interconnectivity of Euroclear Bank with other FMIs is a critical component in the Euroclear Group strategy to establish a common pool of collateral assets in which Euroclear Group entities provide collateral management services as a triparty agent taking over the collateral management tasks (including collateral selection, valuation and substitution) from its participants during the lifecycle of the transaction concluded between two participants. At the end of 2017, at group level, the average daily value of triparty collateral managed by the Euroclear (I)CSDs reached € equivalent 1.150 trillion (up from € 1.072 trillion in 2016).

(1) Settlement currencies (February 2018): AED, ARS, AUD, BGN, BHD, BWP, BRL, CAD, CHF, CLP, CZK, CNY, DKK, EUR, GBP, GHS, HKD, HRK, HUF, ISK, IDR, ILS, JOD, JPY, KES, KWD, KZT, LBP, MAD, MUR, MXN, MYR, NAD, NGN, NOK, NZD, OMR, PEN, PHP, PLN, QAR, RON, RUB, SAR, SEK, SGD, THB, TND, TRY, USD, ZAR.

(2) Denomination currencies (February 2018): DZD, AOA, AMD, AZN, BDT, BYR, BMD, BOB, KHR, XOF, XAF, CLF, COP, CRC, DOP, EGP, GEL, XAU, GTQ, INR, JMD, KGS, MKD, MNT, MXV, MZN, MMK, NPR, TWD, NIO, PKR, PYG, RWF, XDR, RSD, KRW, LKR, TZS, TTD, TMT, UGX, UAH, UYU, UZS, VUV, VEF, VND, YER, ZMW.

SECURITIES DEPOSITS AND SETTLEMENT TURNOVER IN EUROCLEAR BANK



Source: Euroclear.

Supervisory priorities in 2018

One of the main priorities for 2018 is the CSDR authorisation filing of Euroclear Bank and Euroclear Belgium. The Bank has set deadlines for Euroclear Belgium and Euroclear Bank to provide additional information in order to complete their CSDR filing (i.e. September 2018 and December 2018 respectively). Key in the assessment will be the governance of the Euroclear Group and the role of Euroclear SA/NV as both the owner of and critical service provider to the Euroclear Group (I)CSDs. In that regard, the Bank will continue in 2018 its review of risk governance developments, as parts of risk management are outsourced to Euroclear SA/NV. For NBB-SSS, further oversight work will be conducted with regard to the provision of settlement against payment services in other currencies than EUR, GBP and DKK.

The Bank has several cooperation arrangements with other authorities with regard to Euroclear Group entities (see also table 3 below). Taking into account the Bank's accountability as lead authority, cooperation with other authorities for Euroclear Bank will be further developed, in particular with FSMA and with the Luxembourg authorities (Banque Centrale de Luxembourg/Commission de Surveillance du Secteur Financier). At the same time, a structural review of current arrangements will be conducted as far as cooperation with regard to Euroclear SA/NV is concerned. Under the CSDR,

regulators of the Euroclear Group (I)CSDs have the possibility to interact directly with Euroclear SA/NV as critical service provider of their respective local CSDs. The competent and relevant authorities of the outsourcing CSDs can have access to the information directly from the outsourcee (in this case Euroclear SA/NV) to assess the outsourced activities' compliance with CSDR. While cooperation between Euroclear Group regulators remains warranted (e.g. exchange outcome of Euroclear Group regulators' assessments), new working arrangements will focus on the exchange of information among regulators, in particular for areas of common interest at group level (i.e. governance, risk management, cyber resilience, outsourcing). Similarly, in line with the CSDR, cooperation in the framework of ESES has evolved from a joint assessment by ESES authorities to a coordination of national assessments by each ESES authority.

In parallel with the preparation of the CSDR authorisation process, the Bank will update its assessment of Euroclear Bank against the PFMIs by consulting and considering the views of the members of the Multilateral Oversight Group. As from 2018, this process will be based on self-assessments conducted by Euroclear Bank.

High priority continues to be set on cyber security in the Euroclear Group entities subject to the Bank's supervision and oversight (i.e. Euroclear SA/NV, Euroclear Bank and Euroclear Belgium). Initiatives to further enhance Euroclear's cyber security posture will continue to be followed up closely, as will its adherence to SWIFT's Customer Security Programme (see chapter 4). Work in this field is done in cooperation with other Euroclear Group regulators in the framework of the Cyber Security Task Force.

The Bank continues to monitor trends in activity that might change the risk profile of the (I)CSDs subject to supervision and oversight (e.g. FinTech initiatives, potential evolution in collateral management services following the implementation of EMIR).

TABLE 3 COOPERATION BETWEEN THE BANK AND OTHER AUTHORITIES WITH REGARD TO EUROCLEAR

	Rationale for cooperation
National cooperation	
FSMA	Market authority responsibilities regarding CSDs in Belgium
International cooperation	
Euroclear SA/NV	
Euroclear Group overseers and market supervisors (BE: NBB, FSMA; FI: Bank of Finland, Finanssivalvonta; FR: Banque de France, Autorité des marchés financiers (AMF); NL: De Nederlandsche Bank (DNB), Autoriteit Financiële Markten (AFM); SE: Riksbank, Finansinspektionen; UK: Bank of England, Financial Conduct Authority)	Multilateral cooperation with regard to the parent holding company of the Euroclear Group (I)CSDs (Euroclear SA/NV), a critical service provider to the Euroclear Group entities
Euroclear Bank	
Central banks of issue of major currencies in Euroclear Bank (Federal Reserve System, Bank of England, Bank of Japan and European Central Bank as observer)	Multilateral cooperation with the relevant central banks of issue of the major currencies settled in Euroclear Bank (i.e. €, $, £ and ¥)
European Central Bank	Bilateral cooperation in the framework of oversight and financial stability within the euro area
Bank of England	Bilateral cooperation on specific aspects of Euroclear Bank relevant for Bank of England
Bank of Japan	Bilateral cooperation on specific aspects of Euroclear Bank relevant for Bank of Japan
Central Bank of Ireland	Bilateral cooperation with regard to the outsourcing settlement of Irish bonds in Euroclear Bank
Hong Kong Monetary Authority	Bilateral cooperation focusing on the links between Euroclear Bank and Hong Kong market infrastructures
Banque Centrale de Luxembourg / Commission de Surveillance du Secteur Financier (CSSF)	Bilateral cooperation on the oversight and supervision of the ICSDs Euroclear Bank and Clearstream Banking Luxembourg
Securities Exchange Commission	Bilateral cooperation focusing on US-related activities within Euroclear Bank
ESES	
ESES overseers and market supervisors (BE: NBB, FSMA; FR: BdF, AMF; NL: DNB, AFM)	Multilateral cooperation covering the CSDs of Euroclear France, Euroclear Nederland and Euroclear Belgium sharing a common rulebook

Source: NBB.

2.3 Custodians

Changes in regulatory framework

Hosting institutions with significant custody activities worldwide, supervision in Belgium has always taken a specific approach, complementing the banking supervision framework, in order to tackle all relevant risk dimensions of custody activities in an appropriate way. This approach is being further formalised with a new category of "assimilated institution".

Before, there was only one category; i.e. "institutions assimilated with settlement institutions" providing, in whole or in part, the operational management of services provided by settlement institutions (e.g. Euroclear SA/NV). The new Law of 31 July 2017 introduced as a new category credit institutions with activities exclusively in the following areas: custody, bookkeeping and settlement services in financial instruments, as well as associated non-banking services, in addition to receiving deposits or other repayable funds from the public and granting credit for own account[1] where such activities are ancillary or linked to the above-mentioned services. Both categories of assimilated institutions have a very similar profile.

In addition, the main activity of this new category of assimilated institutions is holding (off-balance) financial instruments on behalf of their clients. As the banking supervision framework does not address prudential supervision aspects of this type of activity (i.e. client asset protection, intraday liquidity, etc.), a specific prudential supervision approach on those areas not covered by the banking regulations (and therefore outside the scope of the SSM[2]) is warranted. The ECB issued a favourable opinion on the creation of such new category of credit institutions assimilated to settlement institutions to which the Bank may apply supervisory tools akin to those applied to international and domestic CSDs[3].

Another set of rules relevant for institutions providing custody services are those of ESMA for the reporting on settlement internalisers within the context of the CSDR published in March 2018. A settlement internaliser refers to an institution that makes transfer orders on behalf of clients or on its own account other than through a securities settlement system. The purpose is to identify institutions not considered as a securities settlement system transferring financial instruments on their own books without instructing the CSD. This is possible when both the seller and the buyer of one trade are clients with the same intermediary institution offering safekeeping services. It is also possible for institutions having both the seller and the buyer of one trade as clients to still instruct the CSD simply because they have not created an infrastructure for internal settlement.

On behalf of ESMA, national competent authorities collect information on settlement internalisers in their jurisdictions. For the Bank, institutions within scope are (i) settlement internalisers established and operating in Belgium; (ii) branches in Belgium of non-EU settlement internalisers; (iii) branches (in other Member States) of settlement internalisers established and operating in Belgium. According to Article 9.1 of the CSDR, settlement internalisers have to report to the competent authorities of their place of establishment on securities transactions they settle outside securities settlement systems. The March 2018 ESMA Guidelines for settlement internalisers clarify the scope of the data to be reported and the types of transactions and operations that should or should not be included.

(1) Activities referred to in Article 1, § 3, first indent of the Banking Law.
(2) Within the meaning of Regulation (EU) No. 1024/2013 of 15 October 2013 conferring specific tasks on the ECB concerning policies relating to the prudential supervision of credit institutions http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:287:0063:0089:EN:PDF.
(3) https://www.ecb.europa.eu/ecb/legal/pdf/en_con_2017_23_signed.pdf.pdf.

Prudential approach

The supervision of custodian institutions followed three classical lines of approach: (1) "baseline supervision" covering SREP but also recovery and resolution, (2) "event-driven supervision" focusing on the analysis of business projects (including follow-up of the new status of assimilated institution), and (3) "risk-based supervision" including client asset protection issues, platforms transformation (i.e. mergers, upgrades and resiliency enhancements) and treasury activities (i.e. treasury management, treasury services and payments).

These approaches are implemented through different (often combined) types of action depending on the subject matter. These include quantitative and qualitative analysis of strategic and financial developments as well as their impact on the institution's risk profile, and deep-dives into various risks and processes whose assessment in terms of contribution to the risk profile may be underestimated by the institution. In addition, the Bank's experts were involved in inspection assignments and their follow-up, as well as in various international colleges, workshops and crisis exercises.

Acting as global custodian of the BNYM Group, BNYM SA/NV has a strong international dimension as illustrated in box 4 (see also its governance structure in Annex 2). It falls under the direct supervision of the SSM. The majority of planned actions by the Bank are therefore carried out within the SSM framework.

Supervisory priorities in 2018

Priorities for prudential supervision in the area of custodians will focus on implementing business projects to enable transition of those institutions' business models to a post-Brexit environment. These projects include in particular the transfer into the EU of activities no longer benefiting from passporting rights as currently enjoyed by the UK, a revision of back-to-back booking models[1] and outsourcing arrangements, the adaptation of the Risk Management and Control Framework, and more broadly operational resilience, organisation and governance in the new context. The robustness of the projects will be assessed not only from the point of view of day-to-day business but also throughout the crisis management continuum (crisis management, recovery and resolution).

The Bank has to identify the institutions to be qualified as settlement internalisers within the meaning of the CSDR. Should institutions be identified as such, a specific reporting needs to be set up.

(1) When a given (set of) market positions of an institution is reversed towards the group in a way that is perfectly matching (couples of transactions have opposite risk positions and all their other features are identical), there is as such no open position for the institution that does not bear the risk linked to those transactions anymore.

Box 4: International dimension of Bank of New York Mellon Group and SA/NV

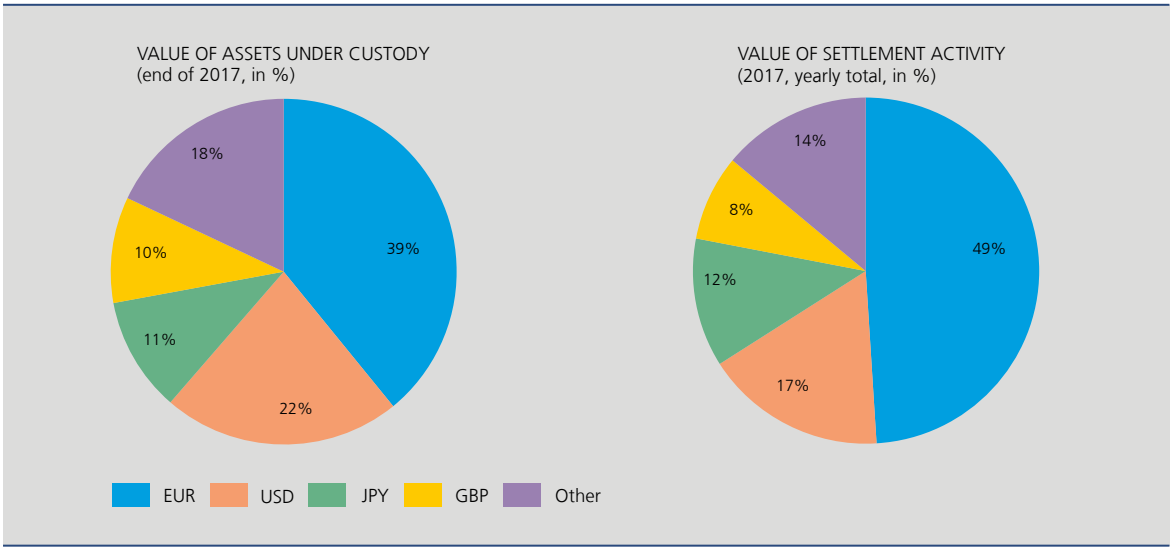
The Bank of New York Mellon, a banking group incorporated in the US, is the largest custody bank in the world in terms of assets under custody ($ 33.3 trillion as of March 2018). It is a global systemically important institution (G-SIB), providing asset and investment management services to institutional clients. The Bank of New York Mellon SA/NV (BNYM SA/NV), the Belgian subsidiary, provides asset services only and acts as global custodian for the banking group through its international sub-custodian network with more than 100 securities markets. BNYM SA/NV has a non-bank subsidiary in Germany and branches in the UK, Luxembourg, the Netherlands, Germany, France, Ireland and Italy through which it operates in these local markets. BNYM SA/NV qualifies as a domestic systemically important financial institution (D-SIFI) following the BCBS criteria or, based on the related EBA guidelines as an other systemically important institution (O-SII).

By the end of 2017, BNYM SA/NV served more than 1 800 international, institutional clients on whose behalf it held € 3.6 trillion equivalent assets under custody (from close to € 3.5 trillion last year), denominated in more than 80 different currencies[1]. The main part of these assets is in EUR (39 %), followed by USD (22 %), JPY (11 %) and GBP (10 %). In terms of settlement activity[2], BNYM SA/NV processed about 15.5 million transactions worth € 43.9 trillion equivalent in 2017. The main currencies are EUR (49 %), USD (17 %), JPY (12 %) and GBP (8 %).

(1) Eligible currencies include AED, ARS, AUD, AZN, BDT, BGN, BHD, BMD, BRL, BSD, BWP, CAD, CHF, CLP, CNY, COP, CRC, CZK, DKK, EGP, ETB, EUR, FKP, GBP, GHS, GMD, HKD, HRK, HUF, IDR, ILS, INR, ISK, JOD, JPY, KES, KRW, KWD, KYD, KZT, LBP, LKR, MAD, MUR, MXN, MYR, MZN, NAD, NGN, NIO, NOK, NZD, OMR, PEN, PGK, PHP, PKR, PLN, PYG, QAR, RON, RSD, RUB, SAR, SEK, SGD, THB, TND, TRY, TWD, TZS, UAH, UGX, USD, UYU, VEF, VND, XOF, ZAR, ZMW, ZWL.

(2) Volume and value of BNYM SA/NV settlement activity is based on receipt and delivery instructions.

ASSETS UNDER CUSTODY AND SETTLEMENT ACTIVITY IN BNYM SA/NV BY CURRENCY



Source: BNYM SA/NV.

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.

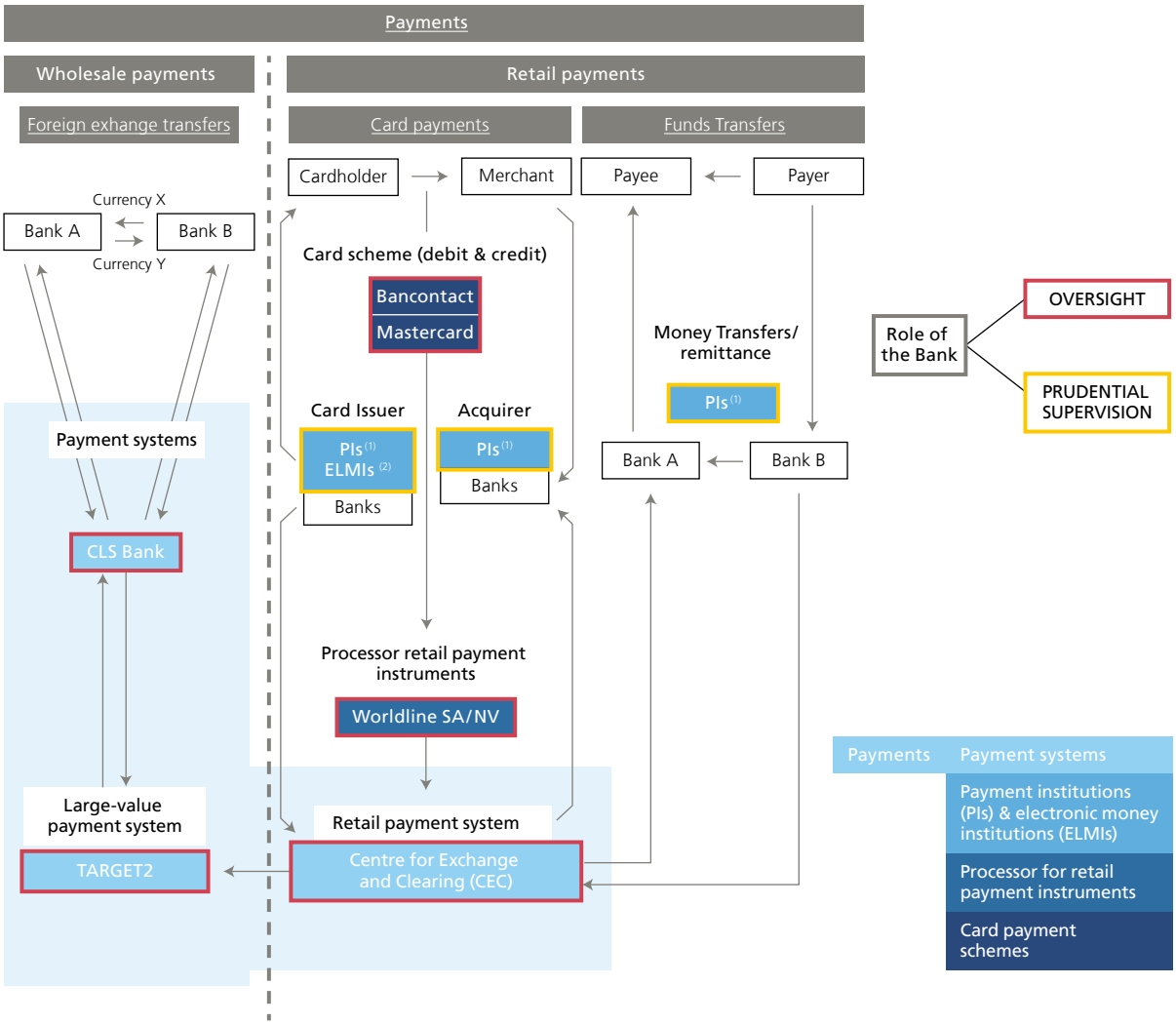
Prudential supervision of payment institutions (PIs) and electronic money institutions (ELMIs) – a new sector of PSPs which may offer since 2009, just like banks, payment services in Europe – is described in section 3.2. This category of non-bank PSPs for retail payments provides respectively payment 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, Loyaltek 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 consultating 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 the 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 inherence (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

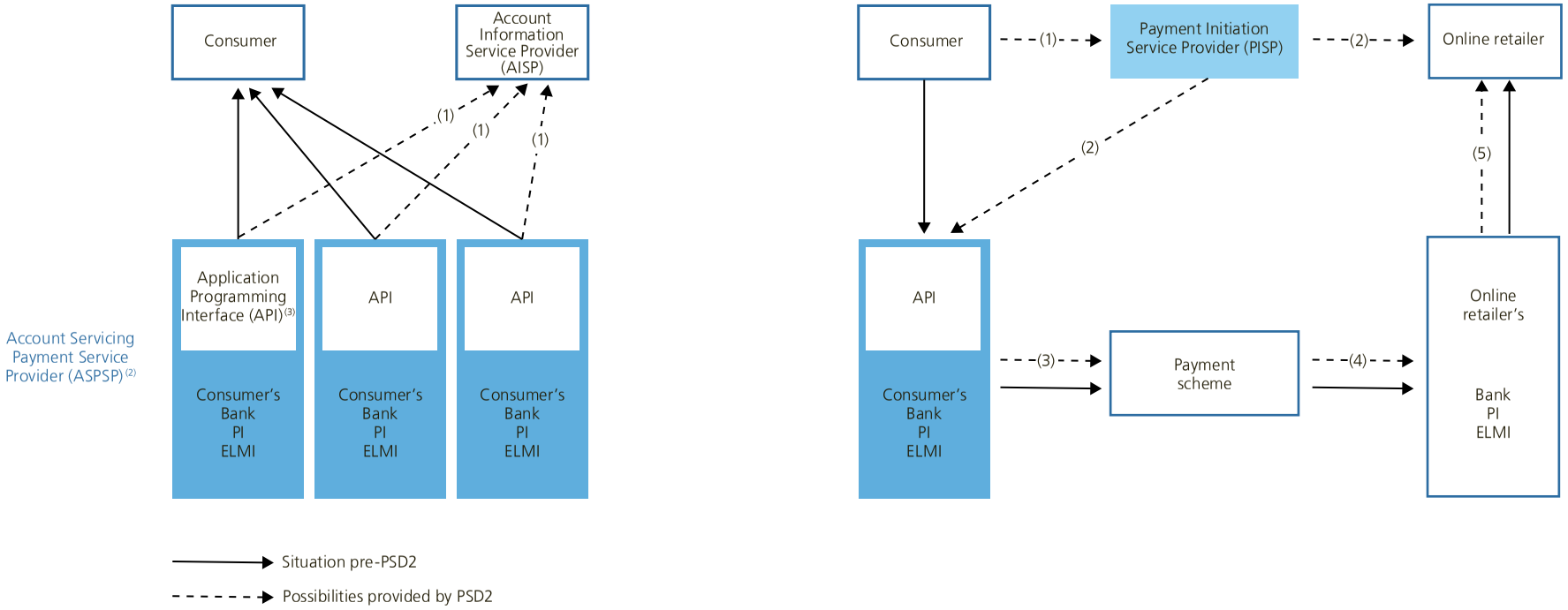
THIRD PARTY PROVIDER (TPP)(1)

ACCOUNT INFORMATION SERVICE PROVIDER (AISP)

Whereas a consumer used to consult all its financial institutions (Bank, PI, ELMI) pre-PSD2 to obtain a global statement of account information, it can now aggregate account information from different ASPSPs (1) via a single AISP (2)

PAYMENT INITIATION SERVICE PROVIDER (PISP)

Whereas a consumer used to initiate payments via its financial institution pre-PSD2, it can now use a PISP (1) to initiate a payment to its online retailer (2). Once the ASPSP instructs the payment scheme (3), next stages of the payment process (4,5) remain unchanged



(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.

Source: NBB.

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

CHART 1 : BELGIAN PIS AND ELMIS
(cumulative number, end of year)

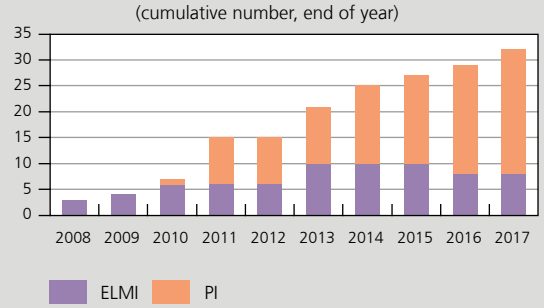


CHART 2 : OTHER EEA PIS' AND ELMIS' BRANCHES IN BELGIUM
(cumulative number, end of year)

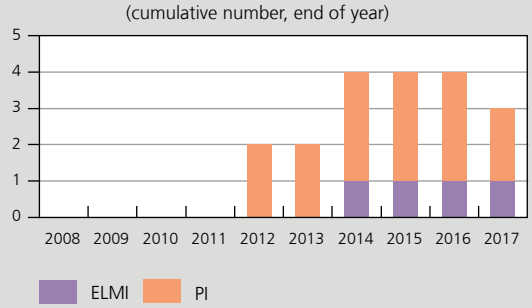


CHART 3 : NUMBER AND VALUE OF TRANSACTIONS BY BELGIAN PIS AND ELMIS
(yearly total) (1)

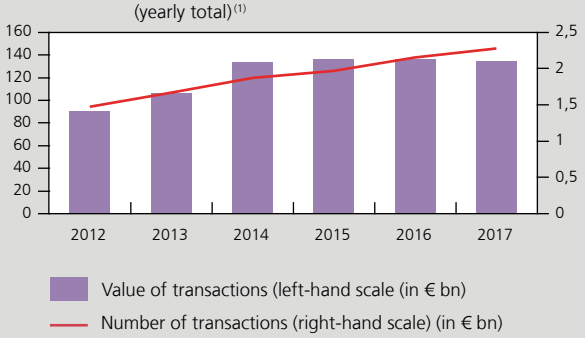
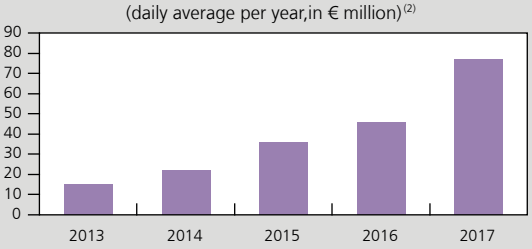


CHART 4: AVERAGE OUTSTANDING E-MONEY OF BELGIAN ELMIS
(daily average per year,in € million) (2)



PASSPORT NOTIFICATIONS FOR CROSS BORDER SERVICES

CHART 5 : BELGIAN PIS AND ELMIS TOWARDS OTHER EEA COUNTRIES
(cumulative number, end of year)

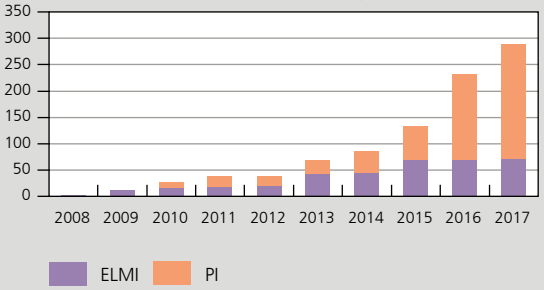
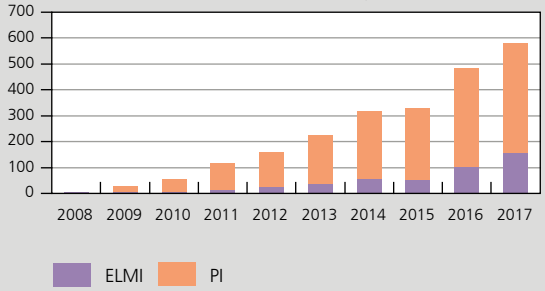


CHART 6 : OTHER EEA PIS AND ELMIS TOWARDS BELGIUM
(cumulative number, end of year)



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.

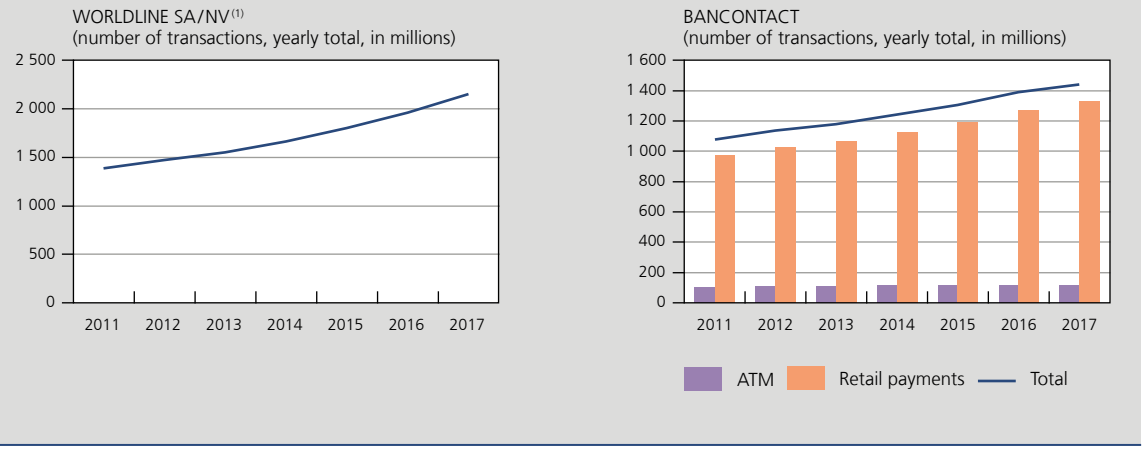
Following the investment of the Worldline Group in Equens SE (NL), which entailed the contribution in kind of Worldline SA/NV's processing business unit in the Dutch Automated Clearing House, Equens subsequently changed its name to equensWorldline SE. Its activities encompass the operation of the Dutch 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

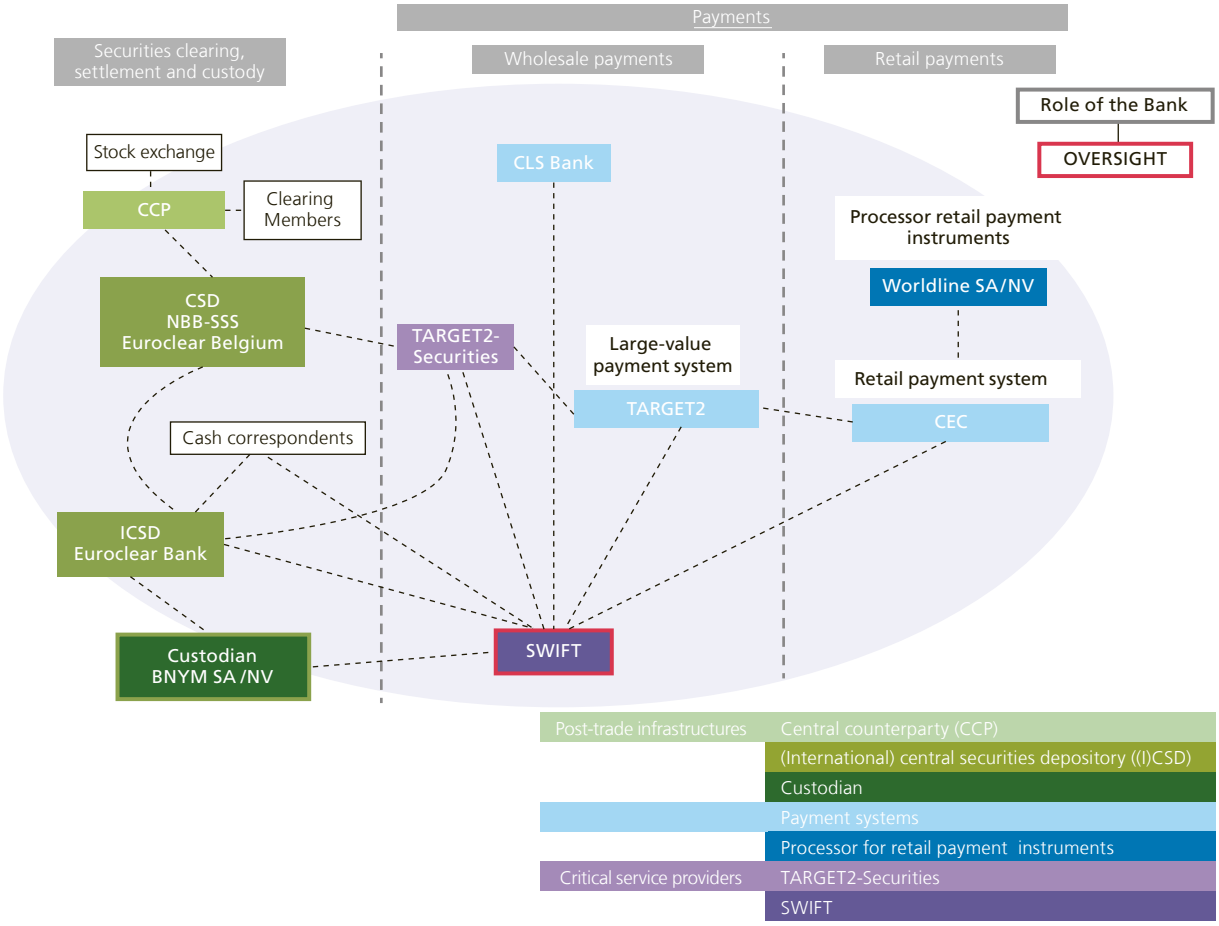
(1) Eurosystem Oversight Framework for Card Payment Schemes – Standards (January 2008) and Guide for the assessment of card payment schemes against the oversight standards (February 2015).
(2) Above the minimum threshold set in the Eurosystem Oversight Framework for Card Payment Schemes – Standards (January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

4. SWIFT

The Society for Worldwide Interbank Financial Telecommunication (SWIFT) is a limited liability cooperative company registered in Belgium that provides messaging and connectivity services to both financial institutions and market infrastructures. These customer types are characterised by their diversity in terms of activities and size, e.g. SWIFT serves banks, brokers, investment managers, fund administrators, trading institutions, treasury counterparties and trusts.

CHART 5 SWIFT AS CRITICAL SERVICE PROVIDER TO THE FINANCIAL INDUSTRY AND THE BANK'S OVERSIGHT ROLE



Source : NBB.

Given its systemic importance as critical service provider to global correspondent banking activities and financial market infrastructures (see chart 5), SWIFT is itself of systemic importance.

Oversight approach

As SWIFT's messaging activities are critical to the smooth functioning, safety and efficiency of major payment and securities settlement systems worldwide (see box 8), the central banks of the G10 agreed to make SWIFT subject to cooperative central bank oversight.

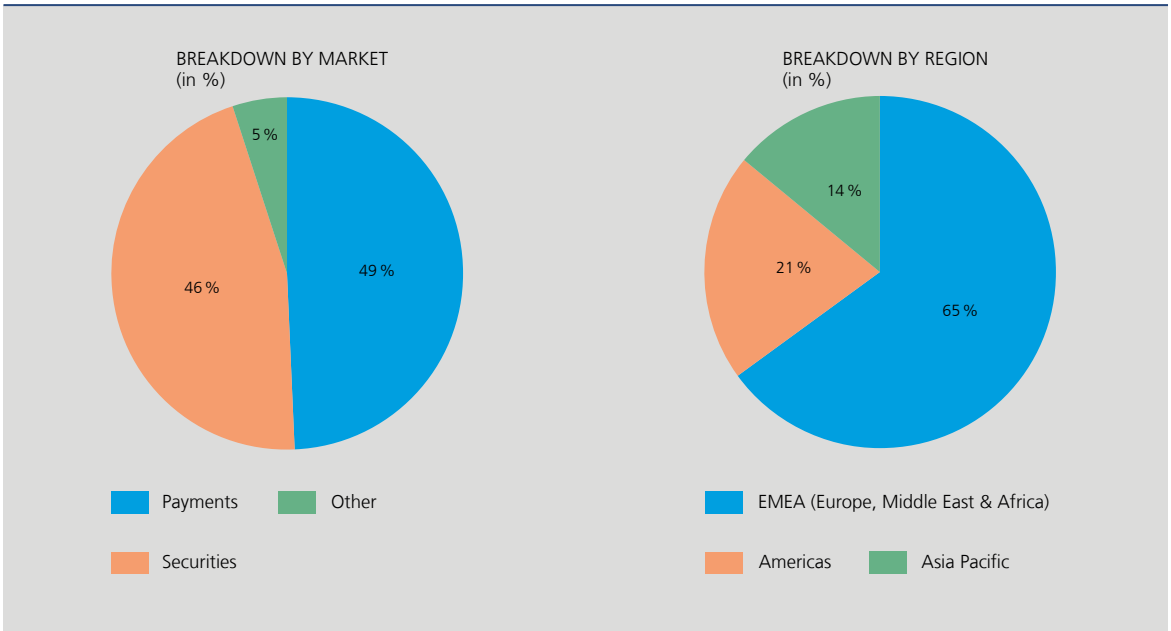
By jointly interacting with SWIFT and formulating joint recommendations concerning it, central banks aim to raise efficiency of their actions as well as the effectiveness of SWIFT's own actions taken in response to their recommendations. Because SWIFT is incorporated in Belgium, the Bank acts as the lead overseer in cooperation with the other G10 central banks. Complementary to this arrangement, a structure is in place to inform the senior overseers from the G20 countries about SWIFT oversight conclusions. The group also discusses oversight policy vis-à-vis SWIFT. An overview of the oversight set-up can be found in box 9.

Box 8 – International dimension of SWIFT

SWIFT is owned and controlled by its members. It has an ongoing dialogue with its customers through national member groups, user groups and dedicated working groups. These discussions relate, for example, to SWIFT's activities such as proposals for new or revised standards, providing industry comments on proposed corporate or business service changes, and comments on timeframes for new technology or service implementation.

SWIFT FIN ACTIVITY

(2017, based on yearly total)



Source: SWIFT.

Each member holds shares proportional to its use of SWIFT's message transmission services. Every three years, a share reallocation is implemented to reflect changes in each member's use of SWIFT. The next reallocation will take place at the 2018 annual general meeting based on 2017 full-year traffic data. Countries or country constituencies propose directors to the Board according to the number of shares owned by all members in the country.

SWIFT's customers are located in more than 200 countries and territories: there are 11 336 live customers of which 2 382 are shareholding members. FIN is SWIFT's core messaging service for exchanging financial messages. Total FIN traffic volume in 2017 reached 7.08 billion messages (+8.4 % compared to the previous year), i.e. about 28.14 million messages per day. These messages flow between participants in stock exchanges, payment systems, (I)CSDs and CCPs. SWIFT FIN traffic in 2017 was 49 % related to payments and 46 % to securities messaging (see chart below, left-hand panel), The main part of the traffic originated from EMEA members (65 %), followed by those from the Americas region (21 %) (right-hand panel).

Box 9 – The international cooperative oversight of SWIFT

As lead overseer, the Bank conducts the oversight of SWIFT in cooperation with the other G10 central banks (i.e. Bank of Canada, Deutsche Bundesbank, European Central Bank, Banque de France, Banca d'Italia, Bank of Japan, De Nederlandsche Bank, Sveriges Riksbank, Swiss National Bank, Bank of England and the Federal Reserve System, represented by the Federal Reserve Bank of New York and the Board of Governors of the Federal Reserve System).

The Bank monitors SWIFT developments on an ongoing basis. It identifies relevant issues through the analysis of documents provided by SWIFT and through discussions with the management. It maintains a continuous relationship with SWIFT, with regular *ad hoc* meetings, and serves as the G10 central banks' entry point for the cooperative oversight of SWIFT. In that capacity, the Bank chairs the senior policy and technical groups that facilitate the cooperative oversight, provides the secretariat and monitors the follow-up of the decisions taken.

The various SWIFT oversight groups are structured as follows:

- the SWIFT Cooperative Oversight Group (OG), composed of all G10 central banks, the ECB and the chairman of the CPMI, is the forum through which central banks conduct cooperative oversight of SWIFT, and in particular discuss oversight strategy and policies related to SWIFT;
- within the OG, the Executive Group (EG) holds discussions with SWIFT's Board and management on the central banks' oversight policy, issues of concern, SWIFT's strategy regarding oversight objectives, and the conclusions. The EG supports the Bank in preparing for discussions within the broader OG, and represents the OG in discussions with SWIFT. The EG can communicate recommendations to SWIFT on behalf of the OG. At one of the EG meetings, the annual reporting by SWIFT's external security auditor is discussed. The EG includes the Bank of Japan, the Federal Reserve Board, the Bank of England, the ECB and the Bank;
- at the technical level, the SWIFT Technical Oversight Group (TG) meets with SWIFT management, internal audit and staff to carry out the groundwork of the oversight. Specialised knowledge is needed to understand SWIFT's use of computer technology and the associated risks. The TG draws its expertise from the pool of staff available at the cooperating central banks. It reports its findings and recommendations to the OG.

The SWIFT Oversight Forum is composed of senior overseers from the G10 central banks (OG) and 10 additional central banks (i.e. Reserve Bank of Australia, People's Bank of China, Hong Kong Monetary Authority, Reserve Bank of India, Bank of Korea, Central Bank of Russia, Saudi Arabian Monetary Agency, Monetary Authority of Singapore, South African Reserve Bank and Central Bank of the Republic of Turkey). Its objectives are to:

- facilitate a coordinated flow of information about SWIFT oversight conclusions to the Forum participants;
- foster discussions on the oversight policy concerning SWIFT;
- provide input to the OG on priorities in the oversight of SWIFT;
- serve as a communications platform on system interdependencies related to the common use of SWIFT or for communication in the event of major contingency situations related to SWIFT.

The framework for the oversight of SWIFT is provided by the five High Level Expectations (HLEs) that focus particularly on the adequate management of operational risks[1]. The framework establishes the common terminology within which oversight discussions can be held. These expectations vis-a-vis SWIFT have evolved into generic oversight requirements for all critical service providers to FMIs, and were included as Annex F in the CPMI-IOSCO Principles for FMIs. SWIFT periodically reports to the overseers on its compliance with the HLEs, which is one of the starting points for identification and further analysis of the risk drivers at SWIFT. Enterprise risk management, information security and technology risk management have been standing topics in the oversight discussions with SWIFT.

Under this framework, the overseers devoted considerable time in 2017 to monitoring SWIFT's Customer Security Programme, and its Global Payments Innovation that aims to increase the transparency and speed of cross-border payment message flows. Overseers also reviewed the expanding portfolio of SWIFT services, e.g. in the area of compliance with financial crime regulation. In the fourth quarter of 2017, the IMF reviewed the SWIFT oversight arrangements in the context of a Financial Sector Assessment Program (FSAP) mission to Belgium (see box 10).

SWIFT's Customer Security Programme aims to strengthen the security of the global financial community against cyber threats by providing guidance to the customers in terms of how they should secure their own local IT infrastructure used for connecting into SWIFT. In addition to this guidance and establishment of a framework to foster increased transparency amongst SWIFT users on customers' adherence to the guiding controls, the programme also focuses on making additional tools available to customers to assist them in preventing and detecting fraud in commercial relationships. Furthermore, under the programme, SWIFT is taking various initiatives for sharing information, thus enabling customers to better prepare for resisting any future cyber threats.

Overseers monitored the significant progress made in 2017 in the first area of the Customer Security Programme ("secure and protect"). In April 2017, SWIFT published its Customer Security Controls Framework introducing a set of mandatory and advisory controls applicable to all customers. After customer consultation and overseers' review, SWIFT explicitly specified – for each control – the objectives and the risks to be addressed. The increased focus on control objectives now allows customers to demonstrate compliance with specific controls through an alternative method, other than the one originally described in the SWIFT controls implementation, as long as the risks identified are mitigated.

All SWIFT customers were required to assess and attest their compliance status against each of the applicable mandatory security controls by the end of 2017. Their self-attestations are collected in a registry that will be used as of 2018 to improve transparency of a SWIFT customer's compliance status vis-à-vis its counterparties. SWIFT customers will be encouraged to take this compliance information into account during their counterparty due diligence reviews. Greater transparency in the SWIFT user community on compliance with security controls is thus a key design feature

(1) The HLEs for the oversight of SWIFT cover (1) risk identification and management, (2) information security, (3) reliability and resilience, (4) technology planning and (5) communication with users.

of the strategy aimed at creating peer-driven pressure to strengthen security. Overseers requested additional security assessments of the registry of attestations itself, and asked SWIFT to consider the development of further action plans if the goals of the current strategy based on transparency amongst customers are not met. Potential issues that need to be monitored might include a limited number of submitted customer attestations and/or low levels of compliance with the controls.

Additionally, SWIFT reserves the right to report customers that did not attest – and, as of January 2019, customers that are non-compliant with the mandatory controls – to their supervisory authority. This escalation process has been reviewed by the overseers.

The overseers also informed SWIFT that they want to be kept informed on relevant metrics to monitor the effectiveness of the customer security controls and attestations. Overseers furthermore continue to follow up on the hardening of the interfaces used by customers to connect to SWIFT, be they installed in their local SWIFT environments or provided by a service provider. They also reviewed the rolling out of SWIFT's Information Sharing and Analysis Centre (ISAC) and the establishment of the Customer Security Intelligence team. Additionally, overseers examined the design and implementation of new financial crime compliance messaging solutions like daily validation reports and payments control and sanctions screening service.

Whereas overseers' monitoring on the further development of the SWIFT Customer Security Programme is inspired by a broad focus on financial stability for the wider ecosystem comprised of SWIFT and its customers, the oversight focus still remains on the security and availability of SWIFT's own operations. Here, too, a major focus is on cyber security matters.

In 2017, the overseers concentrated on the design, implementation and testing of processes for cyber event detection, monitoring and response. Highlights in this area of interest include the review of the multi-year roadmap for further improving the cyber security posture of SWIFT and the review of results of logical intrusion tests and more sophisticated types of penetration testing. Once a year, the overseers also challenge the external security auditor on its opinion and the findings and observations underpinning that opinion.

Interface products for customer connection to SWIFT are not only provided by SWIFT, but also by third parties. Rather than installing such interfaces on their premises, customers can also connect to SWIFT via a service provider (a 'service bureau' or 'shared infrastructure provider'). Overseers not only focused on the Customer Security Programme described earlier, but also reviewed the (cyber) risk mitigation strategies applied by SWIFT to third-party providers of interface products (through a SWIFT certification programme) and shared infrastructure providers. At the request of the overseers, SWIFT aligned the cyber security requirements of the shared infrastructure programme with those of the Customer Security Programme, the latter providing the minimum-security baseline for shared infrastructure. For example, operators of shared infrastructures must comply with both the mandatory and the advisory controls of the Customer Security Programme.

SWIFT's long-term strategy and how it aligns with specific platform investments are regularly discussed with representatives of SWIFT's management and Board. Overseers typically challenge such plans on the aspects of security and strategic focus.

Overseers conduct regular evaluations of the effectiveness of the various lines of defence and governance structures, for daily operations, long-term strategies and specific projects. Specific attention is paid to the development and implementation of the enterprise risk management (ERM) roadmap and the recurring assessment of extreme risks and recovery plans. Overseers are closely monitoring how SWIFT is continuing the build-up of a truly integrated ERM framework that also pays due attention to other types of risk than technical or security risks.

When incidents take place in SWIFT's infrastructure, network or operations, the overseers investigate the sequence of events, analyse the customer impact, and review the results of the investigation. Detailed action plans that outline the activities, deadlines and responsibilities within SWIFT are requested where necessary. There is frequent follow-up on these action plans, designed to prevent recurrence of similar incidents.

Box 10 – IMF recommendations on the oversight of SWIFT

The IMF FSAP mission conducted in the fourth quarter of 2017 in Belgium covered the oversight of SWIFT. The IMF issued three recommendations:

1. Consider a regulatory backstop to complement the current moral suasion basis of the SWIFT oversight;
2. Consider broadening the membership of the SWIFT Oversight Forum;
3. Improve information sharing on SWIFT oversight and assurance reports.

On the first recommendation, legal reviews will be conducted to investigate how moral suasion can be combined with a regulatory backstop. On the expansion of the SWIFT Oversight Forum, contact will be made with additional central banks, inviting them to sign a Memorandum of Understanding with the Bank to join the Forum. The review of criteria determining which central banks will be invited will be discussed with current Forum members. On the increased transparency on SWIFT oversight and SWIFT assurance reports, various initiatives will be undertaken, either by the Bank itself through publications or through meetings and conferences involving relevant stakeholders (e.g. other central banks or financial authorities) or by encouraging SWIFT to make existing assurance reports better known amongst relevant authorities and/or amongst its customers themselves.

Oversight priorities in 2018

The primary oversight focus remains the adequacy of SWIFT's cyber strategy for protecting the infrastructure, networks and operations under its control. This includes the review of the updated multi-year cyber security roadmap and progress in its roll-out. Additionally, the findings – if any – of the external security auditor will be analysed and potential remediation discussed.

Overseers will ask SWIFT to obtain info about relevant metrics to monitor the effectiveness of the Customer Security Programme. Attention will be paid to the level of compliance with the security controls, to validating the current control mix (relevance of current controls, advisory versus mandatory controls), and the effectiveness of the attestation and reporting processes as enforcement mechanisms. When needed, the overseers will request – and review – remediation plans.

These major areas of focus are complemented with continuous monitoring activities structured in line with the HLEs. Firstly, continuous monitoring in the context of the risk identification and management expectations will focus on further development of the ERM methodology and risk acceptance processes, as well as further refinement of the risk registry. The overseers periodically assess the effectiveness of the three lines of defence, i.e. self-assessment of risks by line management, assessments by the independent risk management function, and reviews by internal audit.

Secondly, business continuity processes and disaster recovery strategies will be assessed against the requirements specified in the CPMI-IOSCO guidance on cyber resilience.

Thirdly, overseers plan a series of risk evaluations for strategic IT options and possible future technology renewals. Furthermore, the overseers will review the potential impact of these technology innovations on the confidentiality, integrity and availability of information. Due attention will be paid to review vendor, patching and incident response processes.

Fourthly, the overseers will examine the improvements to the communication processes to inform customers. In the light of recent cyber incidents caused by compromised customer environments, overseers will analyse the functioning of the Customer Security Intelligence team and the distribution of actionable cyber threat information via SWIFT's ISAC.

Additionally, the roll-out of the Customer Security Programme processes for reporting non-compliant customers will be examined and challenged where necessary.

Finally, the overseers continue to analyse the design and follow-up on the implementation of major projects that could significantly impact the risk profile of SWIFT.

Specific theme : Endpoint security : a comparative overview of approaches to reduce payment fraud

Filip Caron

Significant developments are apparent in the cyber threat landscape of the global financial industry. Sophisticated adversaries have been acquiring – and successfully exploiting – detailed knowledge on the business processes and IT infrastructure needed to conduct payments. While the 2016 cyber attack against the Bank of Bangladesh was a watershed moment for the industry, a further refining of the cyber attack vectors is being observed. A coordinated community supported response will be needed.

Forensic analysis of recent cyber incidents in the financial sector has indicated that compromising the endpoints of a payment system to inject fraudulent payments, is a viable strategy for cyber criminals. Sophisticated custom malware has been used to acquire administrator rights, manipulate software in memory, bypass authentication mechanisms, install process monitoring tools and delay incident response by hiding evidence and installing ransomware as a smokescreen.

Recurring payment fraud may expose the ecosystem to risks that have an impact far beyond the financial losses for a compromised endpoint ; it may undermine confidence in the integrity of the payment infrastructure. Participants with concerns about the integrity of the system or the implications for their own security posture may be tempted to implement controls that further limit payment instruction processing. In a worst-case scenario, these controls could impede economic activity and even threaten financial stability in the case of wholesale payments.

For this article, an endpoint of a payment system, service provider or network is defined as a point in place and time at which payment instruction information is exchanged between parties and their respective information systems. The next section introduces the three established endpoint security initiatives, followed by a comparative analysis of these initiatives in various dimensions. The concluding section discusses the findings and puts forward significant challenges related to the operationalisation of these strategies.

Endpoint security approaches to reduce payments fraud

A wide spectrum of payment arrangements exists in the financial industry, each with a different infrastructural set-up and security needs. Three diverse initiatives that aim to get a grip on endpoint security to reduce payment fraud have received close attention.

– SWIFT's Customer Security Programme (SWIFT's CSP) targeting security among participants of its messaging and network services ;

– The Payment Card Industry Data Security Standard (PCIDSS) developed by the major card schemes (i.e. American Express, Discover Financial Services, JCB International, MasterCard, and Visa Inc.) to establish a data security baseline for all entities involved in payment card processing or the storage, processing or transmission of cardholder data and/or sensitive authentication data;
– Security-related specifications under the Second Payments Services Directive (PSD2), which set security baselines for *payment initiation service providers* (PISP) and payers, and endpoints for the systems of *account servicing payment service providers* (ASPSP) and PISPs respectively.

Each of the initiatives targets a different segment of the payments market, namely interbank payment messages, card payments and internet payments. While all three initiatives aim at mitigating risks related to information security and loss of confidence, there is a financial stability risk dimension for the wholesale payments market, as SWIFT is considered a systemically important service provider for the segment.

The three endpoint security reinforcing initiatives are being sponsored by three significantly different stakeholders: an industry incumbent, an industry council and a regulator. While this indicates that a wide variety of stakeholders may be interested in operationalising an endpoint security strategy, it also suggests opportunities for active cooperation with the private sector.

Furthermore, the endpoint infrastructures considered for an endpoint security reinforcing initiative may vary significantly. SWIFT's CSP focuses primarily on the local SWIFT infrastructure (including the operators and their computers) at their participants, as well as the relevant data flows with back office applications. The security-related specifications under PSD2 cover the full infrastructure of the PISP linked via *application programming interfaces* (APIs) to the ASPSP and the strong authentication mechanisms of the payers. Depending on the presence of compensating controls, de facto effective network segmentation, the scope of the PCIDSS either includes the full network-connected infrastructure at the endpoint or is limited to the isolated cardholder data environment (i.e. people, processes and technologies used for the storage, processing and/or transmission of cardholder data or sensitive authentication data).

The Basel Committee for Payments and Market Infrastructures (CPMI) recently presented a general strategy for reducing the risk of wholesale payments fraud related to endpoint security, more details can be found in box 1.

Strategic elements in payment fraud reduction

The comparative analysis of the endpoint security initiatives will focus on four aspects: mechanisms for increasing security baselines for endpoints, mechanisms for promoting the reinforcement of endpoint security, tools for fraud prevention and detection and fraud response procedures. As the validation of PCIDSS compliance may vary depending on the payment card scheme, this comparative analysis is based on MasterCard's approach to endpoint security.

Increasing security baselines for endpoints

Recent cyber incidents revealed important security weaknesses at the endpoints of payment service providers, making them the perceived weakest link in the payment chain and a suitable target for cyber criminals. As a result, improving the security baselines for endpoints could be a viable objective for a payment fraud reduction initiative.

There are various potential options for improving the security baseline for endpoints, including the prescription of hard technical requirements, mechanical enforcement of security enhancements such as automatic mandatory updates, targeted awareness campaigns and principle-based security requirements. Specifying challenging but attainable security requirements has been the preferred option in each of the three initiatives.

Box – CPMI Strategy for reducing the risk of wholesale payments fraud related to endpoint security

In response to the growing threat of wholesale payment fraud, which may undermine confidence in the integrity of the entire system, the Basel Committee on Payments and Market Infrastructures (CPMI) developed a strategy to encourage and help focus industry efforts towards reducing the risk of wholesale payments fraud related to endpoint security.

The **strategy** addresses all areas relevant to payment fraud prevention, detection, response and (external) communication. Seven strategy elements provide a high-level overview of the actions needed.

1. ***Identify and understand the range of risks*** faced by the various actors in the ecosystem, including payment system operators, networks and participants. In addition to security risks faced by individual actors, there are risks faced collectively such as a potential loss of confidence in a payments system;
2. ***Establish endpoint requirements*** that specify a minimum-security baseline for all payment system and network participants;
3. Processes to ***promote adherence*** should ensure that all payment system and network participants comply with the endpoint requirements;
4. ***Provide and use information and tools to improve prevention and detection*** which would enhance the participants' capabilities to prevent and/or detect in a timely manner wholesale payment fraud attempts;
5. Define standardised practices to ***respond in a timely way to potential fraud***;
6. ***Support ongoing education, awareness and information-sharing***;
7. ***Learn, evolve and coordinate.***

While being descriptive and thereby allowing for the necessary flexibility, the CPMI has distilled points for consideration from experienced stakeholders' comments. These points for consideration could assist other operators, participants and relevant stakeholders in developing and operationalising their individual endpoint security strategy.

All stakeholders in the wholesale payment ecosystem should take responsibility for their own systems, risk management and internal control frameworks. Concretely, complying with endpoint security requirements does not imply a shift in liability from participants to wholesale payment system or network operators; participants remain responsible for conducting adequate due diligence assessments of counterparties; and participants adopting fraud prevention and detection tools developed by a payment system or network operator remain responsible for accurately parameterising these tools and dealing with the alerts that they generate.

A successful **operationalisation** of the presented strategy will depend on active cooperation between all relevant actors, including payment system operators, participants and public stakeholders. The CPMI is committed to promoting effective and coherent operationalisation of the strategy within and across jurisdictions and systems. CPMI member central banks will act as catalyst for the effective and coherent operationalisation of the strategy within and across jurisdictions and systems, monitor progress throughout 2018 and 2019, and where necessary take action to ensure adequate progress in the operationalisation of the strategy. That action includes encouraging the establishment of responsibilities and timelines, as well as identifying significant obstacles and/or opportunities (e.g. for cross-system coordination or harmonisation). The Cooperative Oversight of SWIFT, and the Bank as the lead overseer, follow up on the implementation of SWIFT's Customer Security Programme, an advanced operationalisation of the strategy.

The strategy is relevant for several risk management topics covered in the CPMI-IOSCO Principles for Financial Market Infrastructures (PFMIs); Annex F of the PFMIs on oversight expectations for critical service providers; and

the CPMI-IOSCO guidance on cyber resilience for financial market infrastructures. The strategy is not intended to replace or supersede them.

References:
- https://www.bis.org/cpmi/publ/d178.htm.
- https://www.nbb.be/nl/artikels/central-banks-urge-industry-wide-take-strategy-improve-wholesale-payments-security.

The security requirements in the three initiatives, which together form the security baseline for endpoints, are generally well grounded in internationally accepted information security standards such as the ISO/IEC 27002 and the NIST Cybersecurity Framework. Control objectives are adapted to the endpoint security context and cover the prevention of payment fraud (e.g. effective network segregation, strong access control, system hardening, penetration testing and security awareness campaigns); the detection of payment fraud (e.g. implementation of intrusion detection systems, software/data base integrity checking and payments control); and response to detected payment fraud (e.g. specifying incident response plans). While the actual security requirements are relatively comparable across initiatives, the focus varies slightly. Examples of individual focal points include the transmission and storage of critical information in PCIDSS, network segregation in SWIFT's CSP and governance and risk management in the context of PSD2. An overview of the high-level control objectives per initiative can be found in Table 1.

TABLE 1 OVERVIEW OF THE HIGH-LEVEL CONTROL OBJECTIVES

SWIFT's CSP	PCI-DSS	PSD2
1. Restrict internet access & protect critical systems from general IT environment	1. Build and maintain a secure network and systems	1. Governance
2. Reduce attack surface and vulnerabilities	2. Protect cardholder data	2. Risk assessment
3. Physically secure the environment	3. Maintain a vulnerability management programme	3. Protection
4. Prevent compromise of credentials	4. Implement strong access control measures	4. Detection
5. Manage identities and segregate privileges	5. Monitor and test networks	5. Business continuity
6. Detect anomalous activity in systems or transaction records	6. Maintain an information security policy	6. Testing of security measures
7. Plan for incident response and information sharing		7. Situational awareness and continuous learning
		8. Payment service user relationship management
		9. Strong customer authentication
		10. Secure communication

Principle-based specifications of endpoint security requirements are mostly preferred over prescriptive control implementations outlining how a participant should comply with an endpoint security requirement. These principle-based specifications allow participants to design controls that are practical, appropriate and effective given the unique attributes of their system.

All three initiatives claim a principle-based approach; however, the requirements in the PCIDSS tend to be more prescriptive than those formulated by the European regulators in the context of PSD2. For example, the European regulators specify that PISPs should establish and implement preventive security measures against identified operational and security risks (e.g. firewalls), and that these measures should be implemented in a defence-in-depth approach. In contrast, the PCIDSS and SWIFT – respectively in the requirements and implementation guidelines sections – go as far as specifying a maximum interval between the review of firewall rules. Another subtle difference in the requirements of the various initiatives is their level of strictness for a similar level of prescriptiveness. For example, under the PCIDSS the firewall rules need to be reviewed every six months, while SWIFT's guidelines stipulate an annual review.

The initiatives provide for proportionality mechanisms, which might mean a distinction between mandatory and advisory controls or differentiated requirements based on specific characteristics of the endpoints. SWIFT adopted both types of proportionality mechanism in its CSP. While the majority of the 27 security requirements are mandatory, SWIFT proposes 11 best practices as advisory security requirements. Additionally, connectivity aggregators providing access to the SWIFT network for third parties need to comply with both mandatory and advisory controls, in contrast to other customers. PCIDSS provides for additional controls for service providers and entities using specific technologies or infrastructural artefacts (e.g. the encryption protocol SSL/early TLS). Within the context of the PSD2, the European regulators allow for several exemptions from strong customer authentication, e.g. for contactless payments at point of sale, low-value transactions, or payments identified as low risk by a suitable transaction monitoring mechanism.

Promoting the reinforcement of endpoint security postures

Endpoint security requirement specifications should be complemented with adequate processes for ensuring adherence to these requirements. There are many possible approaches, including transparency to various stakeholders, mandatory audits, mechanical enforcement, disconnection, or regulatory requirements.

Transparency on the endpoint security posture of participants aims at creating peer-driven momentum to strengthen endpoint security. Participants can take this information into account when conducting counterparty risk assessments, potentially resulting in additional due diligence activity or counterparty-risk-mitigating measures (e.g. limiting amounts or allowed transaction types). There are various potential approaches to transparency : in a scheme with active transparency, endpoint security information is automatically passed on to all known counterparties, whereas in a scheme with passive transparency, counterparties should request access to this information. Additionally, the sponsor of an endpoint security initiative could establish a process to inform the relevant supervisory authorities of (sustained) endpoint security issues, which may result in supervisory pressure on the non-compliant participant.

Sometimes, adherence to an endpoint security requirement could be achieved through mechanical enforcement. For example, a payment service operator could discard messages sent from an endpoint system that does not support two-factor authentication or has not been patched adequately. In a more extreme scenario, a payment service provider, system or network may even opt to disconnect a participant in the event of sustained non-compliance with the requirements. Mechanical enforcement and disconnection enforcement approaches demand action from the payment service provider, system or network, whereas in a transparency-based approach the stakeholders are requested to make risk-informed decisions.

While mechanical enforcement is always based on evidence collection (i.e. automatic screening or auditing/certification), sponsors of an endpoint security initiative may decide on a self-attestation process to collect information regarding the endpoint security posture of a participant. The latter can be complemented with assurance reports from internal and/or external security auditors.

SWIFT has opted for a peer-driven transparency model and requests its users to self-attest on an annual basis. Participants could demand – on a peer-to-peer basis – access to the endpoint security self-attestation of their counterparties. Furthermore, SWIFT has reserved the right to inform relevant supervisory authorities on self-attestation information.

PISPs must provide their competent authority with regular assessment of both the operational and security risks related to their service and the adequacy of the risk mitigation measures. Article 95(2) of the PSD2 prescribes that these assessments will be provided on an annual basis or at shorter intervals if specified by the competent authority. Regarding the link between PISPs and their endpoints, the regulatory technical standard on strong customer authentication and secure communication stipulates that the relevant security measures should be periodically tested and audited by operationally independent IT experts. Audit reports should be provided to the competent authorities upon their request.

While the PCI Security Standards Council (PCI SSC) is responsible for maintaining the PCIDSS and related programmes (including the assessment training and programmes), the enforcement mechanisms are specific to each payment card scheme. Depending on the type of endpoint (primarily driven by the number of transactions), MasterCard requires annual onsite assessments or annual self-assessments (under certain circumstances with transparency towards acquiring institutions). In addition, quarterly network scans by external providers of tested and PCI approved vulnerability scanning services are required.

Designing methods for payment fraud prevention and detection

Fraud prevention and detection tools could further reduce the likelihood and impact of payment fraud. The tools envisaged by the sponsors of the endpoint security initiatives can be divided into four broad categories: reconciliation, strong authentication, statistical analysis, and artificial intelligence applications.

Recent cyber incidents clearly indicated the popularity of transaction log manipulation to conceal payment fraud. Reconciliation tools allow for detecting manipulations of the transaction logs based on independent reports delivered through a separate and secure channel to an endpoint. SWIFT developed the Daily Validation Reports service, which targets smaller participants interested in validating wholesale payments recorded in an endpoint-local transaction database. Certain payment service providers provide similar tools for their respective endpoints, e.g. Worldline offers its participant merchants a reconciliation mechanism as part of its commercial acquiring services.

Strong authentication of an endpoint operator is based on two or more authentication factors, including knowledge factors such as a password; possession factors like owning a token or specific mobile phone number; and inherence factors which are typically biometrics. While there is a significant list of exemptions, PSD2-related security regulation prescribes per default the need for strong authentication. Payment card schemes actively support strong authentication mechanisms. For example, MasterCard requests its issuers to support EMV 3-D Secure 2.0 by the end of 2018, which should be used by its merchants by the end of 2020. SWIFT imposes multi-factor authentication through a mandatory security requirement.

Statistical analysis tools use metrics and related thresholds – formalised in payment policies – to identify potential fraudulent payments. Typical metrics are based on (combinations of) the payment amount, the beneficiaries, and/or the timing/location of the payment instruction's initiation. SWIFT announced a payment control service that allows endpoint operators to specify a payment policy and determine the actions to be taken in the event of an out-of-policy payment instruction. If effective transaction risk analysis is implemented, payment service providers may be exempted from the strong authentication security requirement under PSD2.

Artificial-intelligence-based tools use a variety of recorded data points and expert knowledge to flag potentially fraudulent payments. The algorithms behind MasterCard's Decision Intelligence service examine cardholder behaviour to detect abnormal behaviour and provide a risk score to the issuer. This risk score could influence an issuer's decision to authorise a transaction. As of July 2018, MasterCard will mandate its issuers to enable a transaction alert service that warns cardholders of the potentially fraudulent use of their card. Acquirers are recommended to opt for a merchant monitoring solution to avoid the processing of illegal and brand-damaging transactions. It should be noted that endpoint operators in the various initiatives can always complement mandated tools with a series of other commercially available data analysis tools to enhance their fraud detection.

Given the complexity of these payment fraud detection and prevention tools, there may be a strong incentive to develop them in collaboration with other stakeholders in the ecosystem. For example, MasterCard's Decision Intelligence is a standardised service used by a variety of issuers. Furthermore, fraud detection tools might have specific data requirements that cannot be satisfied by everyone. Reconciliation tools are typically provided by the payment service, system or network operator as they are based on the formal transaction records of that operator (e.g. SWIFT's Daily Validation Reports), which are typically not accessible to other third-party vendors.

Responding to security incidents and payment fraud attempts

Standardised processes and practices to respond to actual or suspected fraud – in a timely manner – should be defined. The objective of these processes should be three-fold, i.e. specifying reporting mechanisms, developing operational responses and distilling actionable cyber intelligence to protect other endpoints.

The regulatory guidelines on major incident reporting under PSD2, addressed to PISPs, specify the criteria, thresholds and methodology to classify operational and security incidents. If an incident is classified as severe, it needs to be reported to the competent domestic authorities using a standardised template within specified timeframes. Furthermore, these guidelines prescribe the criteria that competent domestic authorities could consider in assessing the incidents' relevance

to other authorities and the detail that needs to be shared. Where relevant, cooperation will be promoted between the competent authorities and the EU Agency for Network and Information Security (ENISA).

SWIFT and MasterCard have specified contractual obligations regarding the reporting of security incidents. These contractual obligations cover the preservation of evidence, execution of forensic analyses, and reporting of incidents and findings. Furthermore, standardised procedures to mitigate the loss of individual fraudulent payments have been developed. SWIFT's Standards MT Release 2018 makes it mandatory to include a unique end-to-end tracking (UETR) number in the header of a FIN message. Originally introduced as part of the Global Payment Innovation (GPI) initiative for tracking payments in a payment chain, the UETR enables the establishment of a stop-and-recall procedure (to be launched in 2018). Payment card schemes have standardised rules for fraud-related chargebacks at acquirer and merchant level, which are enforced through both fines and the threat of cancellation of merchant accounts and acquiring licences.

Forensic analysis of security incidents and payment fraud attempts may result in cyber intelligence such as indicators of compromise and attack vectors. Under its CSP, SWIFT established a customer security intelligence team that assists affected customers with forensic investigations. Distilled cyber intelligence is further distributed in SWIFT's community through a dedicated information sharing and analysis centre (ISAC).

Conclusion

The high degree of interconnectedness between financial information systems has been identified as a significant driver of operational, cyber and reputation risk for the operators of individual systems. Connected IT systems at partners are typically not managed by the financial information systems operators, and have proven to be the weakest link in recent cyber incidents involving payment fraud.

Technology risk managers increasingly focus on developing endpoint security initiatives. These initiatives allow for promoting stronger cyber security across all stakeholders, pooling efforts to develop effective payment fraud detection mechanisms, and defining a standardised approach to ensure an effective response to payment fraud.

The comparison of the various initiatives identified a general recurring structure consisting of specifying security requirements, promoting adherence to these requirements, endorsing the use of fraud prevention/detection mechanisms, and prescribing a standardised fraud response. However, different options to operationalise the endpoint strategies have been chosen. A summary can be found in Table 2.

The operationalisation of endpoint security initiatives still faces significant challenges. Stakeholders may fall within the scope of different endpoint security initiatives with conflicting endpoint security requirements. As self-attestation – and the expected peer pressure of transparency on compliance – remains the favourite security requirement adherence promotion method, each stakeholder has to accept its own responsibility. Restrictions concerning data sharing, privacy and law-enforcement may hamper the efficient sharing of cyber threat intelligence. Endpoint security initiatives will have to be carefully reviewed and peer-revised promptly to remain effective in the continuously evolving threat landscape.

TABLE 2 COMPARISON OF THE ENDPOINT SECURITY INITIATIVES

Endpoint security initiative	SWIFT's CSP	PCI-DSS	PSD2
Sponsor	Wholesale payment messaging service and network operator SWIFT	Card payment schemes grouped in the PCI Security Standards Council	European regulators
System-endpoint relationships covered	• SWIFT – SWIFT participants (including financial institutions, corporates and other organisations)	• Acquirer – Merchant • Issuer – Customer • Card scheme – Acquirer • Card Scheme – Issuer • Relationships with third party service providers (e.g. network operators like Worldline, data process and/or storage service providers)	• ASPSP – PISP • PISP – payers
Mechanisms for increasing security baselines for endpoints	• Principle-based security requirements • Advisory controls	• Principle-based security requirements	• Principle-based security requirements formalised in regulation
Mechanisms for promoting the reinforcement of endpoint security	• Self-attestation • Passive transparency to counterparties • Reporting to regulators • SWIFT retains a right to audit	Depending on the payment card scheme and certain parameters, the following mechanisms may be mandatory: • Self-assessment • Annual onsite assessments • Quarterly network scans	• Self-assessments to be provided to the competent supervisory authorities • Mandated periodic testing of security measures • Mandated regular audits by independent IT experts
Tools for fraud prevention and detection	• Included as an advisory control (multi-factor authentication mandatory) • SWIFT specific services offered	• Implementation is mandatory for issuers and acquirers • Payment scheme specific tools and variety of third-party tool providers	• Strong authentication mandatory • Transaction risk analysis might result in exemptions
Fraud response procedures	• Reporting contractually obligatory • Forensic analysis supported by Customer Security Intelligence team at SWIFT • Stop-and-recall mechanism in GPI • Dedicated ISAC	• Reporting, preservation of evidence and forensic analysis may be contractually obligatory for a card scheme	• Strict reporting guidelines • Sharing beyond local authorities under predefined circumstances

Annexes

Annex 1 : Regulatory framework

FMIs	**CPMI-IOSCO Principles for Financial Market Infrastructures (PFMIs) (April 2012) :** International standards for payment systems (PS), central securities depositories (CSDs), securities settlement systems (SSSs) and central counterparties (CCPs). They also incorporate additional guidance for over-the-counter (OTC) derivatives CCPs and trade repositories (TRs). (http://www.bis.org/cpmi/publ/d101a.pdf)
	CPMI-IOSCO Principles for Financial Market Infrastructures, Disclosure framework and assessment methodology (December 2012) : Framework prescribing the form and content of the disclosures expected of FMIs, while the assessment methodology provides guidance to assessors for evaluating observance of the principles and responsibilities set forth in the PFMI. (http://www.bis.org/cpmi/publ/d106.pdf)
	CPMI-IOSCO Recovery of financial market infrastructures (October 2014) : Guidance for FMIs and authorities on the development of comprehensive and effective recovery plans. (http://www.bis.org/cpmi/publ/d121.pdf)
	CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures (June 2016) : Requires FMIs to instil a culture of cyber risk awareness and to demonstrate ongoing re-evaluation and improvement of their cyber resilience posture at every level within the organisation. (http://www.bis.org/cpmi/publ/d146.pdf)
CCPs	**European Market Infrastructure Regulation (EMIR) : Regulation (EU) No 648/2012 of 4 July 2012 on OTC derivatives, CCPs and TRs :** EMIR sets a clearing obligation for standardised OTC derivatives and strict CCP risk management requirements, and requires the recognition and ongoing supervision of CCPs. (http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012R0648&from=EN)
	CPMI-IOSCO Public quantitative disclosure standards for CCPs (February 2015) : Public quantitative disclosure standards that CCPs are expected to meet. These standards complement the Disclosure framework published by CPMI-IOSCO in December 2012. (http://www.bis.org/cpmi/publ/d125.pdf)
	EMIR Regulatory Technical Standards (August 2015) : Regulation (EU) 2015/2205 of 6 August 2015 supplementing Regulation (EU) No 648/2012 with regard to regulatory technical standards on the clearing obligation. (http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R2205&from=EN)

CCPs	**CPMI-IOSCO Resilience of CCPs: Further guidance on the PFMI (July 2017):** Guidance providing further clarity and granularity on several key aspects of the PFMI to further improve CCP resilience. (https://www.bis.org/cpmi/publ/d163.pdf)
CSDs	**CSD Regulation (CSDR): Regulation (EU) No 909/2014 of 23 July 2014 on improving securities settlement in the EU and on CSDs and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012:** Prudential requirements on the operation of (I)CSDs, as well as specific prudential requirements for (I)CSDs and designated credit institutions offering banking-type ancillary services. (http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0909&from=en)
	Regulation (EU) 2017/389 of 11 November 2016 supplementing Regulation (EU) No 909/2014 as regards the parameters for the calculation of cash penalties for settlement fails and the operations of CSDs in host Member States. (http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0389&from=EN)
	Regulation (EU) 2017/390 of 11 November 2016 supplementing Regulation (EU) No 909/2014 with regard to regulatory technical standards on certain prudential requirements for CSDs and designated credit institutions offering banking-type ancillary services. (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0390&from=EN)
	Regulation (EU) 2017/392 of 11 November 2016 supplementing Regulation (EU) No 909/2014 with regard to regulatory technical standards on authorisation, supervisory and operational requirements for CSDs. (http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0392&from=EN)
Custodians	**Regulation (EU) 2017/391 of 11 November 2016 supplementing Regulation (EU) No 909/2014 with regard to regulatory technical standards further specifying the content of the reporting on internalised settlements:** Reporting obligation for settlement internalisers when settlement instructions are executed in their own books, outside securities settlement systems. (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0391&from=EN)
	Belgian law of 31 July 2017: Law introducing a new category of credit institutions with activities exclusively in the area of custody, bookkeeping and settlement services in financial instruments, as well as non-banking services relating thereto, in addition to receiving deposits or other repayable funds from the public and granting credit for own account where such activities are ancillary or linked to the above-mentioned services. (http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=2017073111&table_name=wet/language=fr&la=F&cn=2017073111&table_name=loi)
	ESMA Guidelines on Internalised Settlement Reporting under Article 9 of CSDR (March 2018) (https://www.esma.europa.eu/press-news/esma-news/esma-finalises-guidelines-how-report-internalised-settlement)
Payment Systems	**ECB Regulation (EU) No 795/2014 on oversight requirements for systemically important payment systems (July 2014):** Regulation, based on the CPMI-IOSCO PFMIs, covering systemically important payment systems in the eurozone, large-value and retail payment systems. (https://www.ecb.europa.eu/ecb/legal/pdf/oj_jol_2014_217_r_0006_en_txt.pdf)

Payment Systems	**Revised oversight framework for retail payment systems (RPS) (February 2016):** Revised framework (replacing the one from 2003) identifying RPS categories and clarifying the oversight standards applicable to each category. It also provides guidance on the organisation of oversight activities for systems of relevance to more than one central bank. (https://www.ecb.europa.eu/pub/pdf/other/revisedoversightframeworkretailpaymentsystems201602.en.pdf?bc332d9a718f5336b68bb904a68d29b0)
PIs & ELMIs	**EMD2 (September 2009):** Directive 2009/110/EC of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of ELMIs amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC, *OJ.* 10 October 2009, L. 267, 7-17. (http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0110&from=EN)
	PSD2 (November 2015): Directive (EU) 2015/2366 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. (http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015L2366)
	Belgian Law of 11 March 2018 transposing the PSD2, *Belgian Official Gazette* 26 March 2018. (http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=2018031107&table_name=wet / language=fr&la=F&cn=2018031107&table_name=loi)
Payment Processors	**Belgian Law of 24 March 2017 on supervision of payment transactions processors,** *Belgian Official Gazette* 24 April 2017. (https://www.nbb.be/doc/cp/moniteur/2017/20170424_opp_wet_loi.pdf)
Card Payment Schemes	**Eurosystem Oversight Framework for Card Payment Schemes (CPSs) – Standards (January 2008):** Common oversight policy to promote the reliability of CPSs operating in the euro area, public confidence in card payments and a level playing field across the euro area in a unified market. (https://www.ecb.europa.eu/pub/pdf/other/oversightfwcardpaymentsss200801en.pdf)
	Guide for the assessment of CPS against the oversight standards (February 2015): Assessment guide based on the Eurosystem Oversight Framework for CPSs targeting both governance authorities responsible for ensuring compliance and overseers of CPSs It has been updated by taking into account the January 2013 "Recommendations for the security of internet payments", as well as the February 2014 "Assessment guide for the security of internet payments". (https://www.ecb.europa.eu/pub/pdf/other/guideassessmentcpsagainstoversightstandards201502.en.pdf?499089f7f3aab273925ef6d80767b4a5)
	Regulation (EU) 2015/751 of 29 April 2015 on interchange fees for card-based payment transactions (*OJ.* 19 May 2015, L. 123, 1-15): This regulation contains (i) the definition of a cap for the interchange fees applicable to payment transactions by means of debit or credit cards, (ii) the separation to be put in place between payment card scheme governance activities and processing activities, (iii) measures granting more autonomy to merchants regarding the choice of payment instruments for their clients. (http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R0751&from=EN)
	Belgian law of 1 December 2016 transposing the EU Regulation 2015/751 of 29 April 2015, entitled "Interchange fees for card based payment transactions" (December 2016): *Belgian Official Gazette* 15 December 2016, 86.578. (http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=2016120112&table_name=wet / language=fr&la=F&cn=2016120112&table_name=loi)

Card Payment Schemes	**Regulation (EU) 2018/72 of 4 October 2017 supplementing Regulation (EU) 2015/751 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. (http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R0072&rid=3)
SWIFT	**High level expectations (HLE) for the oversight of SWIFT (June 2007):** The SWIFT Cooperative Oversight Group developed a specific set of principles that apply to SWIFT. (https://www.nbb.be/en/financial-oversight/oversight/critical-service-providers#oversight-of-swift-)
	PFMIs, Annex F: Oversight expectations applicable to critical service providers (April 2012): Expectations for an FMI's critical service providers in order to support the FMI's overall safety and efficiency. (http://www.bis.org/cpmi/publ/d101a.pdf)
	Assessment methodology for the oversight expectations applicable to critical service providers (December 2014): Assessment methodology and guidance for regulators, supervisors and overseers in assessing an FMI's critical service providers against the oversight expectations in Annex F. (http://www.bis.org/cpmi/publ/d123.pdf)

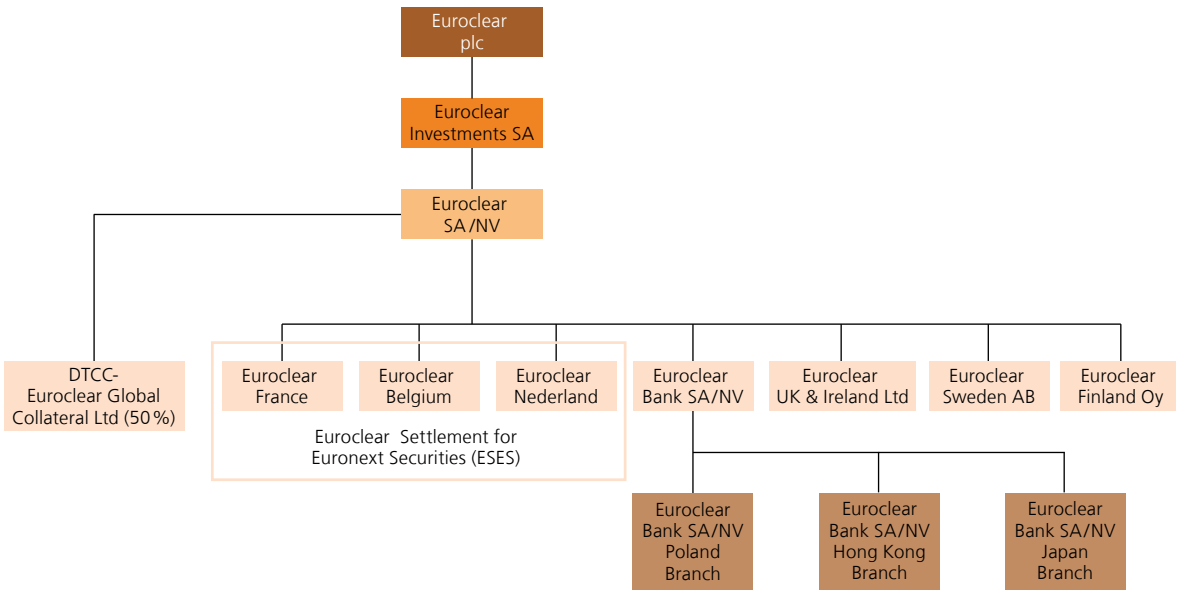
Annex 2 : FMIs established in Belgium with an international dimension

Euroclear

Euroclear SA/NV (ESA), a Belgian financial holding company, is the parent company of the Euroclear Group (I)CSDs : i.e. the CSDs in Belgium, Finland, France, the Netherlands, Sweden, UK & Ireland, and of the ICSD Euroclear Bank. The latter has branches in Poland, Hong Kong and Japan. Euroclear Group (I)CSDs have outsourced the IT production and development to ESA. ESA also delivers common services, such as risk management, internal audit, and legal and human resources services to the Group (I)CSDs. The issued share capital of Euroclear plc, the ultimate holding company of the Euroclear Group, is held mainly by user-shareholders. Euroclear Belgium, Euroclear France and Euroclear Nederland are operating a common settlement platform : i.e. the Euroclear Settlement of Euronext-zone Securities system (ESES). Apart from being owned by the users of its services, the Euroclear Group is also governed

EUROCLEAR GROUP CORPORATE STRUCTURE

(simplified diagram)



Source : NBB.

by its users via their representation on the (Euroclear plc and ESA) Boards. Being user-owned and user-governed, the interests of the user community are represented in the decision-making process of the Euroclear Group. Users can also influence the Euroclear Group's decision-making bodies through the Market Advisory Committees established for each market where an entity of the Euroclear Group acts as CSD, as well as the ESES and Cross-Border Market Advisory Committees. They act as a primary source of feedback and interaction between the user community and Euroclear management on significant matters affecting their respective markets. The Euroclear Group believes this governance structure allows to meet the needs of its participants and markets it serves, taking into account the competitive environment in which it operates.

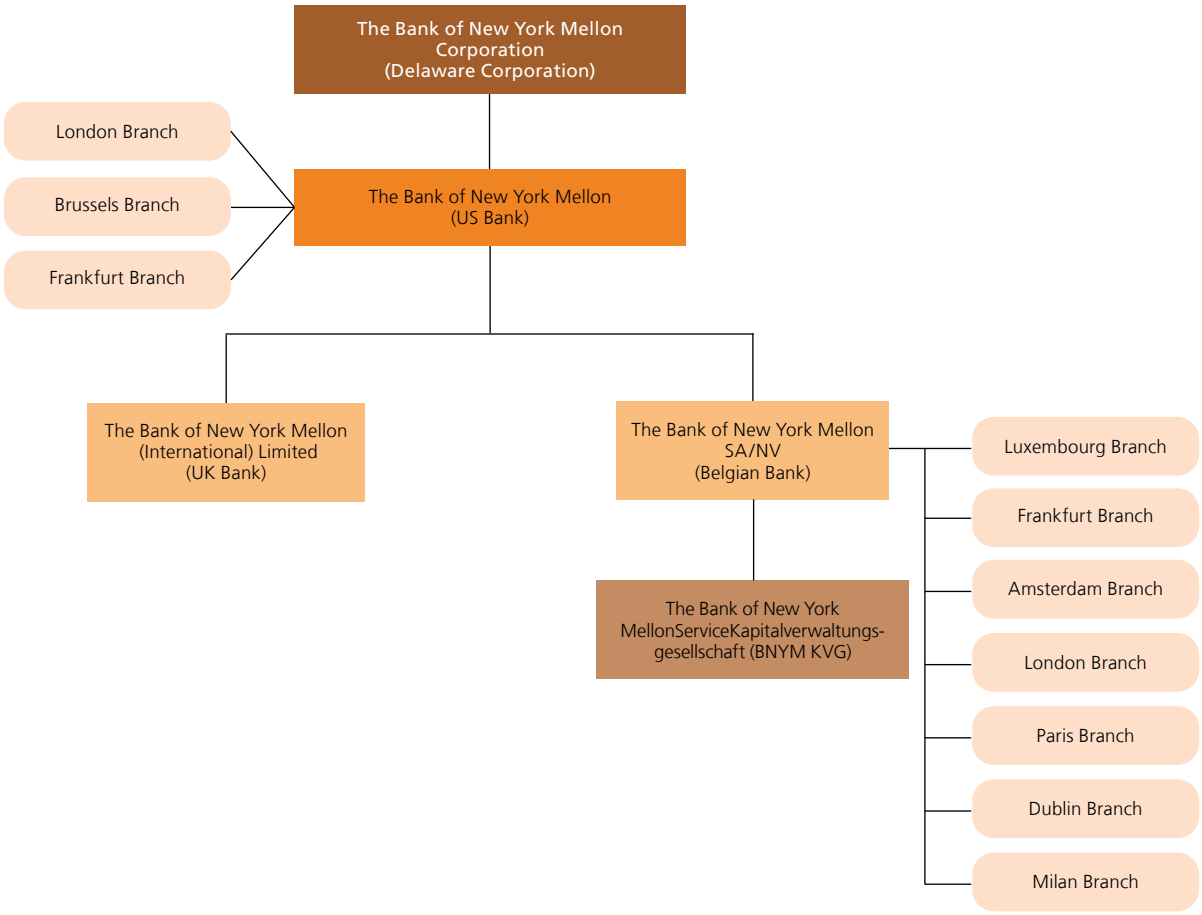
In September 2014, ESA and the US Depository Trust & Clearing Corporation (DTCC) set up the DTCC-Euroclear Global Collateral Ltd. joint venture. The ultimate aim of this entity is to create a joint collateral processing service whereby mutual clients of DTCC and Euroclear Bank manage collateral held at both depositories as a single pool, to meet obligations in both the European and the North American time zone.

Bank of New York Mellon

The Bank of New York Mellon SA/NV (BNYM SA/NV), established in Belgium, is the European subsidiary of BNY Mellon, a US based global systemic bank, which in turn is a subsidiary of the US holding company BNY Mellon Corporation. BNYM SA/NV is the global custodian of the group (i.e. providing investment services on 100+ markets outside the US) and its European gateway to the euro area markets and payment infrastructures. BNYM SA/NV has a non-bank subsidiary in Germany and branches in Luxembourg, Germany, the Netherlands, the UK, France and Ireland and Italy, through which it operates in the local markets. This is the result of the BNYM Group's strategy to consolidate its legal entity structure into the so-called "Three Bank Model" (i.e. US/UK/EU). The BNYM group is also present in Belgium through a branch of the US parent company.

BNYM GROUP STRUCTURE AND BNYM SA/NV POSITION

(simplified diagram)



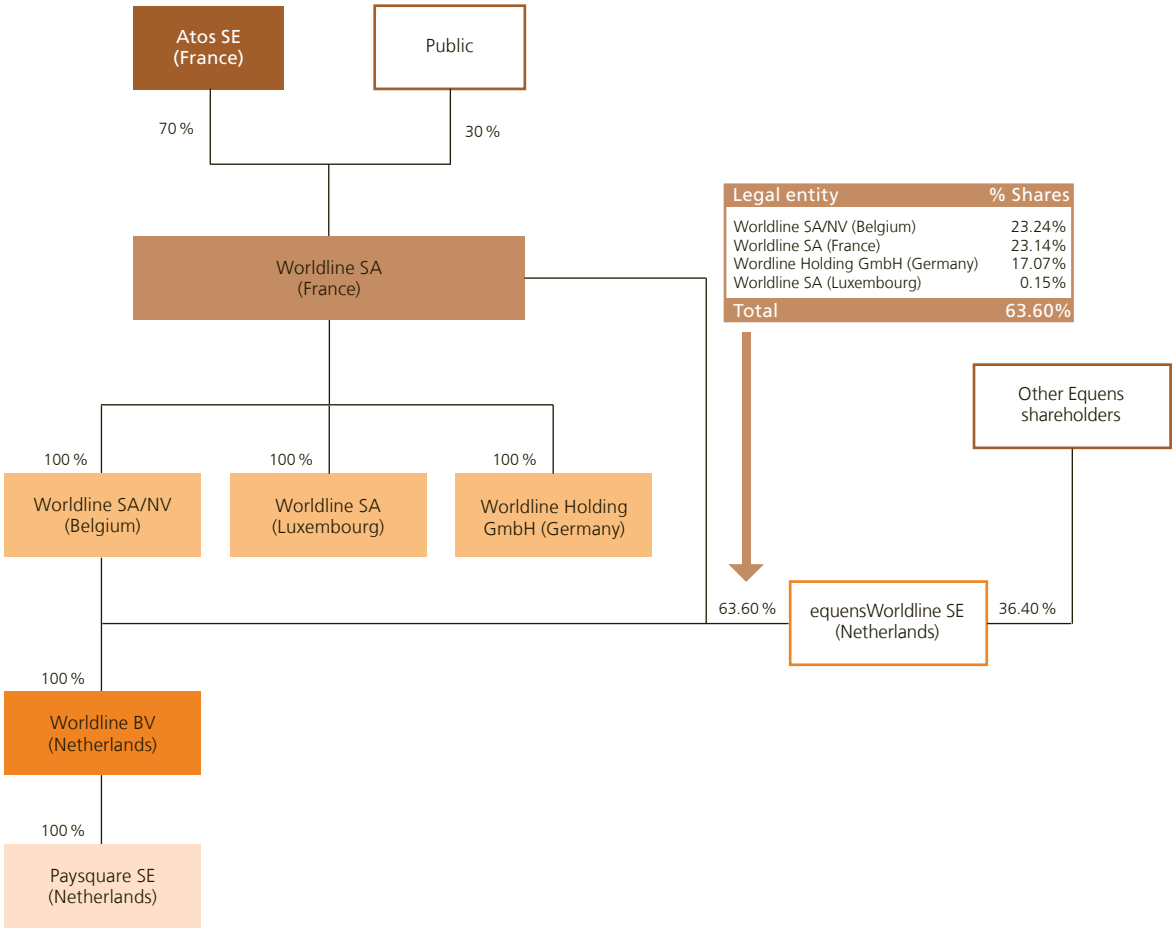
Source: NBB.

Worldline

Worldline, a division of the European IT services corporation Atos, provides electronic payment and transactional services in about 29 countries. It is one of the European leaders in that domain. Worldline SA is listed on Euronext Paris. In 2016, Worldline SA/NV, the Belgian entity of the group merged with the Dutch company Equens. The processing activities were carved out in a new entity called equensWorldline SE. equensWorldline SE is a partial subsidiary of several Worldline entities (Belgium, Luxembourg, France and Germany) with its historic shareholders now as minority shareholders.

STRUCTURE OF WORLDLINE, A DIVISION OF THE ATOS GROUP

(simplified diagram, part of the group relevant for Belgium)



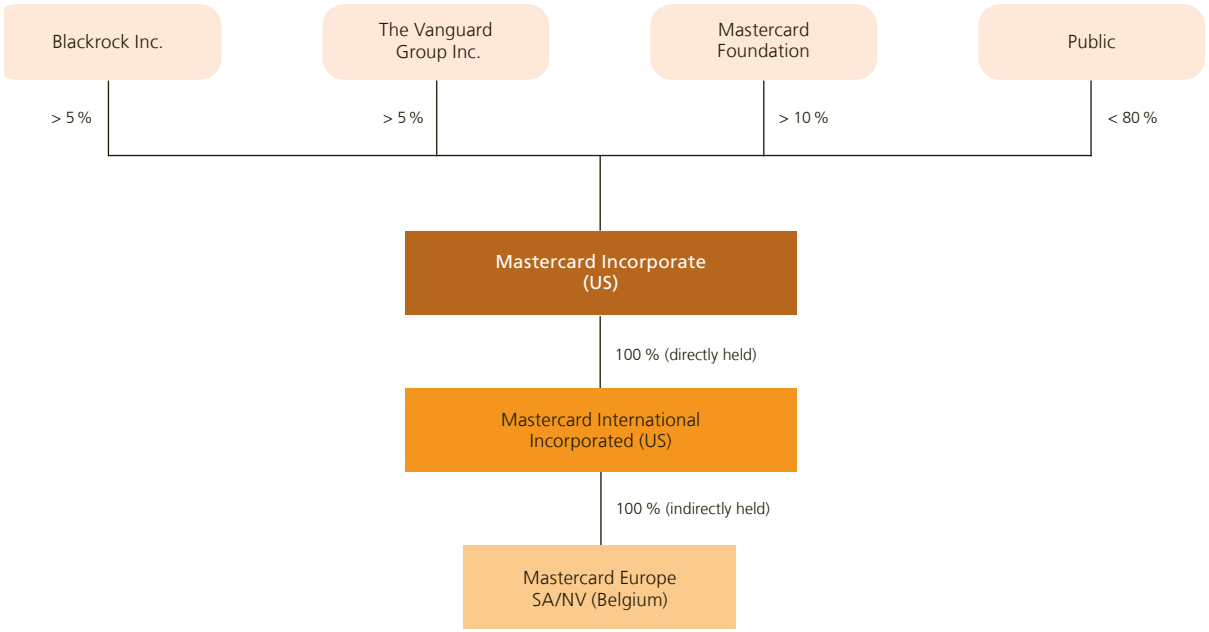
Source: NBB.

Mastercard Europe

Mastercard is a payment services company with a global reach. Mastercard Europe SA/NV (MCE) incorporated in Belgium, a subsidiary of Mastercard Incorporated (US, listed on the New York Stock Exchange), runs the company's business in the European region.

MASTERCARD GROUP STRUCTURE

(simplified diagram)



Source : NBB.

Annex 3 : Statistics

List of tables

TABLE 1 SECURITIES CLEARING, SETTLEMENT AND CUSTODY

(notional value cleared, yearly total in € trillion equivalent)

	2013	2014	2015	2016	2017
A. Central Counterparties (CCPs) (selected)					
LCH.Clearnet Ltd (UK)					
Swapclear (including Interest Rate Swaps, Forward Rate Agreements)	362	503	489	626	807
Repoclear (repos)	40	41	40	37	44
LCH.Clearnet SA (FR)					
Credit Default Swaps (CDSClear)	0.2	0.1	0.2	0.4	0.6
Repoclear (repos)	35	33	33	34	48
Eurex Clearing AG (DE)					
Interest Rate Swaps	0.0	0.1	0.2	0.9	1.4
Repos	97	102	89	65	48

Sources: CCP websites, NBB calculations.

TABLE 1 SECURITIES CLEARING, SETTLEMENT AND CUSTODY (continued)

(yearly total in € billion equivalent, unless otherwise stated)

	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
B. Euroclear Bank										
Value of securities deposits (end of period)	9 135.9	9 832.2	10 453.8	10 766.3	10 837.2	10 834.2	11 765.3	12 393.7	12 698.4	12 834.2
Number of transactions (in millions)	42.0	39.3	47.7	59.4	64.2	69.5	75.2	83.3	84.1	95.4
Value of transactions	282 484.9	219 904.5	265 819.6	328 475.9	307 109.8	336 784.6	394 569.3	442 563.0	451 698.3	498 181.0
Source : Euroclear.										
C. NBB-SSS										
Value of securities deposits (end of period)	408.3	469.3	494.0	513.3	531.2	541.7	557.3	575.4	612.5	625.3
Number of transactions (in millions)	0.3	0.3	0.4	0.5	0.6	0.6	0.6	0.5	0.5	0.5
Value of transactions (1)	8 299.9	7 408.1	9 049.6	14 133.9	10 250.1	8 428.0	8 209.0	8 766.5	8 714.3	9 069.8
Source : NBB.										
(1) Secondary market turnover.										
D. Euroclear Belgium										
Value of securities deposits (end of period)	161.4	139.9	162.0	130.4	156.8	202.7	222.1	269.4	235.1	237.7
Number of transactions (in millions)	2.2	1.9	1.8	1.9	1.9	1.9	2.1	2.5	2.4	2.5
Value of transactions	335.0	398.5	497.7	588.0	563.6	799.8	714.8	944.6	963.8	946.0
Source : Euroclear.										
E. TARGET2-Securities										
Number of transactions (in millions)	nap (2)	nap	nap	nap	nap	nap	nap	7.6	36.3	125.6
Value of transactions	nap	nap	nap	nap	nap	nap	nap	43 706.8	112 066.0	192 175.0
Source : ECB.										
(2) T2S was launched in 2015.										
F. BNYM SA/NV										
Value of assets held under custody (end of period)	nap (3)	2 480.8	2 928.9	2 667.8	2 861.9	2 905.2	3 454.0	3 216.4	3 476.5	3 608.8
Source : BNYM.										
(3) BNYM SA/NV was established in 2009.										

TABLE 2 PAYMENTS

(yearly total in € billion equivalent, unless otherwise stated)

	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
A. TARGET2										
Value of payments	611 134.5	536 027.1	631 440.0	651 274.9	711 025.8	559 696.0	498 726.5	508 982.3	485 811.8	432 780.7
of which: TARGET2-BE	27 123.0	20 835.2	20 199.7	22 163.2	18 712.6	16 177.3	16 247.9	15 627.4	16 957.9	19 732.4
Number of payments (in millions)	89.0	87.8	87.2	89.0	89.6	91.3	87.8	88.6	89.0	89.3
of which: TARGET2-BE	2.7	2.1	2.4	2.6	2.5	2.3	2.5	2.3	2.2	2.3
Source: ECB Payment Statistics. Last year's figures from https://www.ecb.europa.eu/stats/payment_statistics/large_value_payment_systems/html/index.en.html.										
B. CLS Bank										
Value of payments	700 382.6	607 499.9	781 426.9	893 590.4	878 469.0	897 145.6	1 042 062.3	1 118 933.9	1 162 359.8	1 193 728.3
of which: EUR payments	145 636.6	131 665.9	161 791.1	182 482.0	185 881.3	182 305.8	191 170.5	208 555.8	204 370.7	219 924.6
Number of payments (in millions)	136.4	150.1	198.1	206.9	176.6	205.0	204.7	219.1	209.5	198.5
of which: EUR payments	28.1	31.8	42.2	45.5	37.4	36.9	34.4	40.9	34.3	34.0
Sources: ECB Payment Statistics, CLS.										
C. Centre for Exchange and Clearing (CEC)										
Value of payments	803.0	804.9	846.9	886.7	909.1	911.6	870.7	883.4	920.6	941.8
Number of payments (in millions)	1 063.4	1 122.9	1 170.2	1 224.9	1 295.1	1 365.6	1 272.2	1 402.2	1 387.1	1 312.0
Sources: ECB Payment Statistics, NBB.										

TABLE 2 **PAYMENTS** (continued 1)

(end of period, in cumulative number, unless otherwise stated)

	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
D. Payment Institutions (PIs) – Electronic Money Institutions (ELMIs)										
PIs										
Belgian PIs	0	0	1	9	9	11	15	17	21	24
Foreign PIs with Belgian branch	0	0	0	0	2	2	3	3	3	2
Passport notifications for cross-border services										
Belgian PIs towards other EEA countries	0	22	47	104	133	184	262	273	379	421
Foreign EEA PIs towards Belgium	0	0	11	19	19	26	41	65	162	218
ELMIs										
Belgian ELMIs	3	4	6	6	6	10	10	10	8	8
Foreign ELMIs with Belgian branch	0	0	0	0	0	0	1	1	1	1
Passport notifications for cross-border services										
Belgian ELMIs towards other EEA countries	2	12	15	18	19	43	45	69	70	72
Foreign EEA ELMIs towards Belgium	4	7	8	14	28	40	54	53	102	156
Source : NBB.										
E. Payment processors										
Worldline SA/NV										
Number of transactions (yearly total, in millions)	1 175.8	1 230.1	1 295.5	1 387.6	1 473.7	1 553.9	1 665.8	1 790.0	1 964.6	2 149.6
Source : Worldline.										

TABLE 2 **PAYMENTS** (continued 2)

	2011	2012	2013	2014	2015	2016	2017
F. Card transactions							
Number of cards issued by resident payment service providers – Cards with a cash function							
Number of cards (in thousands of numbers, end of period)	20 005.19	20 647.08	20 041.34	21 396.54	21 870.76	22 593.13	nav
Number of cards per capita (end of period)	1.82	1.87	1.80	1.92	1.95	2.00	nav
POS transactions at terminals provided by resident PSPs							
Number of payment transactions per card – With cards issued by resident PSPs (yearly total)	52.41	54.2	60.2	58.4	61.8	67.4	nav
Value of payment transactions per card – With cards issued by resident PSPs (yearly total, in €)	2 752.94	2 838.92	3 091.49	2 906.16	2 948.40	3 094.6	nav
Transactions per capita							
Number of card payments – With cards isssued by resident PSPs[1] (yearly total)	105.15	111.0	120.0	135.2	138.9	151.0	nav
Value of card payments – With cards issued by resident PSPs[1] (yearly total, in € thousands)	5.77	6.1	6.4	6.6	6.9	7.1	nav

Source: ECB Payment Statistics.
(1) Except cards with an e-money function only.

G. Card schemes							
Bancontact – Number of transactions (yearly total, in millions)	1 076.4	1 136.4	1 180.4	1 241.8	1 306.7	1 389.5	1 441.6
of which:							
Retail payments	973.4	1 028.9	1 068.4	1 125.9	1 190.9	1 272.8	1 325.2
ATM	103.0	107.5	111.9	115.9	115.9	116.8	116.3

Source: Bancontact.

TABLE 3 SWIFT

(yearly total, in millions)

	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
Number of messages	3 854.6	3 760.3	4 031.9	4 433.9	4 589.1	5 065.7	5 612.7	6 106.6	6 525.8	7 076.5
of which :										
Payment messages	1 978.6	1 933.9	2 041.4	2 157.5	2 314.4	2 524.5	2 737.2	2 930.2	3 139.3	3 485.2
Securities messages	1 604.3	1 583.5	1 723.2	1 945.9	1 975.3	2 215.6	2 545.2	2 829.1	3 019.1	3 232.3
Other messages	271.7	242.9	267.3	330.5	299.4	325.6	330.3	347.3	367.3	359.0

Source : SWIFT.

List of abbreviations

ACH	Automated clearing house
AISP	Account information service provider
ASPSP	Account servicing payment service provider
BCBS	Basel Committee on Banking Supervision
BNYM	Bank of New York Mellon
BRRD	Bank Recovery and Resolution Directive
CCP	Central counterparty
CEC	Centre for Exchange and Clearing
CLS	Continuous Linked Settlement
CM	Clearing member
CPMI	Committee on Payments and Market Infrastructures
CSDR	CSD Regulation
CSD	Central Securities Depository
D-SIFI	Domestic systemically important financial institution
DTCC	Depository Trust & Clearing Corporation
DvP	Delivery versus payment
EBA	European Banking Authority
EC	European Commission
ECB	European Central Bank
EEA	European Economic Area
ELMI	Electronic money institution
EMD	Electronic Money Directive
EMEA	Europe, Middle East and Africa
EMIR	European Market Infrastructure Regulation
EPC	European Payments Council
ESA	Euroclear SA/NV
ESCB	European System of Central Banks
ESES	Euroclear Settlement of Euronext-zone Securities
ESMA	European Securities and Markets Authority
EU	European Union
FCA	Financial Conduct Authority
FMI	Financial market infrastructure
FSB	Financial Stability Board

FSMA	Financial Services and Markets Authority
FX	Foreign exchange
G-SiFI	Global systemically important financial institution
ICSD	International central securities depository
IFR	Regulation on interchange fees for card-based payment transactions
IOSCO	International Organisation of Securities Commissions
ISAC	Information sharing and analysis centre
LSE	London Stock Exchange
LSI	Less significant institution
MCE	MasterCard Europe
MoU	Memorandum of Understanding
NCA	National competent authority
NCB	National central bank
ORPS	Other retail payment system
O-SII	Other systemically important institution
OTC	Over the counter
PFMIs	CPMI-IOSCO Principles for FMIs
PI	Payment institution
PIRPS	Prominently important retail payment system
PISP	Payment initiation service provider
POS	Point of sale
PSD	Payment Services Directive
PSP	Payment Service Provider
PvP	Payment versus payment
RPS	Retail payment system
RRP	Recovery and resolution planning
SCT Inst	SEPA instant credit transfer
SEPA	Single European Payments Area
SI	Systemically-relevant credit institution
SIPS	Systemically important payment system
SIRPS	Systemically important retail payment system
SSM	Single supervisory mechanism
SSS	Securities settlement system
SWIFT	Society for Worldwide Interbank Financial Telecommunication
T2	TARGET2
T2S	TARGET2-Securities
TTP	Third-party provider

National Bank of Belgium
Limited liability company
RLP Brussels – Company number: 0203.201.340
Registered office: boulevard de Berlaimont 14 – BE-1000 Brussels
www.nbb.be

Publisher

Tim Hermans
Executive Director

National Bank of Belgium
Boulevard de Berlaimont 14 – BE-1000 Brussels

Contact for the publication

Johan Pissens
Deputy Director
Prudential Supervision of Market Infrastructure and Oversight

Tel. +32 2 221 20 57
johan.pissens@nbb.be

Cover and layout: NBB AG – Prepress & Image

Published in June 2018

Printed on FSC paper