Financial Market Infrastructures and Payment Services

Report 2017

National Bank OF BELGIUM
Eurosystem

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

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

Contents

Introduction and executive summary

Belgium hosts a number of significant financial market infrastructures (FMIs), custodians, payment service providers, such as payment institutions (PIs) and electronic money institutions (ELMIs), as well as critical service providers (CSPs), some of which also have a systemic relevance internationally. In recent years, the sector has witnessed a steady increase in activity or new institutions entering the field.

The Financial Market Infrastructures and Payment Services Report provides a comprehensive overview of the National Bank of Belgium's (the Bank) oversight and prudential supervision on these systems and institutions headquartered in, or relevant for Belgium.

The Bank considers such disclosure necessary for a number of reasons.

Firstly, as a financial authority, it should be transparent and accountable about its role, towards the financial sector (as main user of FMIs), and towards the public at large (as user of payment services).

Secondly, as the systems and institutions covered in this Report are an important component for underpinning financial markets as well as the real economy, it is particularly relevant for the participants of FMIs and end users of payment services to be aware of the Bank's view on inherent risks and on priorities for risk mitigation. Similarly, as there is wide variety in the regulatory status of these actors (ranging from credit institutions, to payment systems, card payment schemes, central counterparties (CCPs), central security depositories (CSDs), PIs, ELMIs, etc.), it is important for their participants or end users to have a good understanding of the specific regulatory frameworks that apply to each of them. This is also why the Report devotes attention to the Bank's role with respect to retail payments, as it is relevant for stakeholders and end users to be aware of risks and rules stemming from technological innovations and regulatory changes.

Thirdly, Belgium is home to a number of internationally active FMIs or CSPs, which are also systemically-relevant in other jurisdictions. In these cases, the Bank's oversight and prudential supervision is organised through international cooperative arrangements with foreign central banks and/or regulators. These arrangements are described in this Report. However, some of the FMIs or CSPs have such a wide international range of activities that even authorities which are not part of these cooperative arrangements may be interested in understanding the applicable framework, the regulatory approach and the main priorities.

Finally, in reporting on these activities, the Bank is meeting its requirements with respect to authorities' responsibilities, as laid down in the 2012 Principles for FMIs (PFMIs) of the BIS Committee on Payments and Market Infrastructures (CPMI) and the International Organisation of Securities Commissions (IOSCO). PFMI Responsibility C "Disclosure of policies with respect to PFMIs" states: "Central Banks, market regulators and other relevant authorities should clearly define and disclose their regulatory, supervisory and oversight policies with respect to FMIs".

Until last year, the Bank's disclosure on these matters was spread over the Bank's Annual Report and its Financial Stability Report (formerly Review). It is the Bank's intention to concentrate this information from now on in the Financial Market Infrastructures and Payment Services Report, to be published yearly.

The Report provides an overview of the changes in the regulatory environment for FMIs, custodians, PSPs and CSPs, the development of their activities, the Bank's oversight and prudential supervisory approaches, and its main priorities for 2017.

Since the adoption of the "twin peaks" supervision model in April 2011, the Bank has been responsible for both the oversight of FMIs and prudential supervision of the regulated institutions which operate some of them. The Bank's oversight of payment and settlement infrastructures focuses on the safe and efficient functioning of payment, clearing and settlement systems established in, or relevant, for Belgium. Prudential supervision is intended to ensure that the entities operating market infrastructures are financially robust at microprudential level, thus helping to maintain the confidence of the institution's counterparties and promote financial stability.

In the area of securities clearing and settlement, the international regulatory community has put major emphasis on the clearing obligation for over-the-counter (OTC) derivatives. This has further increased the critical role of CCPs in the financial system, and has led to a further strengthening of the regulatory requirements for CCPs. While there is no CCP established in Belgium, the Bank participates in a number of colleges of CCPs which are relevant from a Belgian perspective.

Belgium is home authority for three CSDs, namely Euroclear Belgium, NBB-SSS and Euroclear Bank (an international CSD or ICSD). The CSD Regulation (CSDR) will be a regulatory milestone in this area as it will increase competition, strengthen regulatory standards and at the same time promote a level playing field by harmonising the supervisory approach. The filing for authorisation of Euroclear Bank and Euroclear Belgium under the CSDR is one of the main supervisory priorities for the Bank.

In the payments area, the Bank supervises sixteen PIs and five ELMIs. The future outlook of this industry is very challenging. On the one hand, a lot of (FinTech) innovation continues to take place within the payment services sector and, on the other hand, the revised edition of the Payment Services Directive (PSD2) is to be transposed into Belgian law by 13 January 2018, introducing, amongst other things, new payment services and harmonised security rules. As acquirer and processor of the majority of debit and credit card payment transactions in Belgium, Worldline SA/NV is subject to both oversight and prudential supervision by the Bank. Because of its systemic relevance, Worldline SA/NV is overseen as a critical infrastructure for payments in Belgium. It also has the supervisory licence of PI given its acquiring business.

As lead overseer of Belgium-based messaging provider SWIFT, the Bank works closely together with other central banks. Over the last few years, a major focus of the oversight has been on cyber risk defence at SWIFT. Recent cyber events have indicated the importance of end-to-end security in the transaction chain. SWIFT has launched a comprehensive programme aimed at reinforcing cyber security among its user community, so-called end-point security. SWIFT will further roll out this Customer Security Programme in the course of 2017. The overseers will follow up on its adequacy and the transparency of communications with users on their own security obligations.

Cyber crime has been on an exponential rise in the last decade, a significant part of which has focused specifically on the financial sector, particularly on FMIs and the payment services sector. This underscores the importance of best practices, proper policy measures and regulatory initiatives such as penetration testing and red team exercises as techniques to acquire reasonable assurance on the effectiveness of an organisation's protection, detection, response and recovery capacities, and the need to share information to cooperate with partners in the financial ecosystem.

The current wave of disruptive technologies and start-ups may open up significant opportunities for the financial industry. At the same time, innovations come with their own set of risks and challenges, including the usual operational (information and cyber), third-party, governance, legal and settlement risks. Regulators strive to promote innovation, security and competition in the financial services industry, while guaranteeing financial stability and a level playing field for all the market participants in terms of risk mitigation and oversight through a risk-based approach that is technology-neutral.

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

The systems and institutions covered in this report form the backbone of the financial ecosystem, either from a wholesale or a retail market perspective, as they are the critical nodes in the functioning of financial markets and payment services. The Bank has, in its capacity of overseer and supervisor, a broad mandate to regulate and supervise them. In order to provide more insight in these systems and institutions' roles, Section 1.1 provides an overview of the structure and interdependencies between these nodes. The relevant processes and flows between nodes and market participants or retail customers 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 the wide range of systems and institutions, either on a national or international basis.

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

Systems and institutions that are the critical nodes in the functioning of financial markets and payment services can in general be put into three categories: (i) securities clearing, settlement and custody, (ii) payments and (iii) critical service providers. Through their activities or services provided to the financial industry, these systems and institutions are interlinked with financial market infrastructures (FMIs), financial institutions and other actors such as merchants or retail customers. These interdependencies, illustrated in chart 1, are further explained below.

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 occur on-exchange, i.e. on a centralised platform designed to optimise the price-discovery process and to concentrate market liquidity. Markets can also function bilaterally or on an over-the-counter (OTC) basis, 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.

Clearing

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.

Settlement

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 act in general 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.

Apart from the type of securities, another distinction between CSDs and ICSDs can be made based on the range of securities that they accept and hold in their systems. Whereas CSDs, as a rule, have so far been operating in a rather domestic environment, ICSDs are – by the very nature of their business model – internationally oriented. They aim to provide their participants with a single gateway to access many local foreign markets (i.e. foreign CSDs which act as notary for securities issued in the local foreign 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". There are three (I)CSDs established in Belgium: Euroclear Bank (ICSD), Euroclear Belgium and NBB-SSS (both CSDs)[3]. The cash leg of securities settlement takes place either in payment systems operated by central banks (i.e. central bank money, e.g. TARGET2) or on the books of an (I)CSD with banking status providing (multicurrency) cash accounts (i.e. commercial bank money, e.g. Euroclear Bank).

Custody

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 is primarily focusing 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 for retail payment instruments and card payment schemes.

Payment systems

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

(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.
(2) The term (I)CSD is used to cover both CSDs and ICSDs.
(3) Bank of New York-Mellon SA/NV indicated that BNYM CSD will not file for a license under the CSD Regulation.

CLS Bank (CLS)[1], a US-based settlement system for foreign exchange (FX) transactions is linked to the RTGS systems operated by central banks of 18 currencies (incl. TARGET2 for EUR) allowing to settle both legs of the FX transaction at the same time. CLS eliminates FX settlement risk whereby – due to time zone differences – one party wires the currency it sold but does not receive the currency it bought from its counterparty.

PIs and ELMIs

Card payments typically involve a "four-party scheme", i.e. cardholder, card issuer, merchant and acquirer. The card of the person who performs the purchase of a transaction with the merchant (cardholder) 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 making the money (paid by the buyer) credited on the account of the merchant). The role of PIs and ELMIs in the retail payments area is multiple ; i.e. for card payments transactions, for example, PIs and ELMIs can issue the payment cards to the user and/or acquire the funds of the payment transaction on behalf of the merchant. The acquiring business has gradually become a market whereby, next to banks, PIs play a growing role.

Next to card payments, PIs have a major role in providing money transfers/remittances services (funds transfers) allowing retail customers to transfer cash from Belgium to a third party in different locations around the world and vice versa.

Processors for retail payment instruments

In Belgium, one specific processor provides the underlying network and services for mainly all card payments, which is Worldline SA/NV. After processing card payments, transactions are sent to the Centre for Exchange and Clearing (CEC) for clearing and settlement.

Card payment schemes

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.

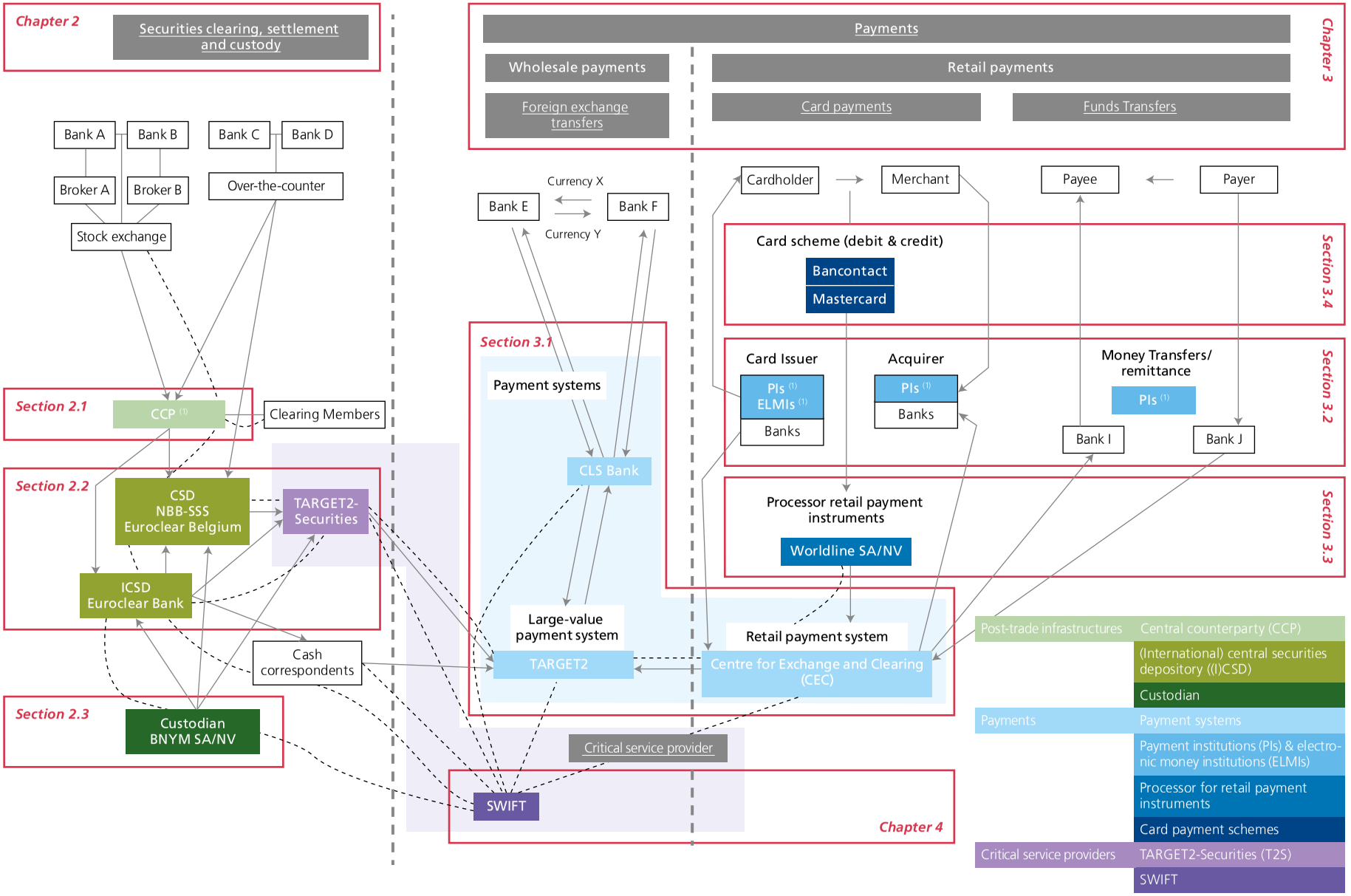
Critical service provider

The report covers two critical service providers (CSPs), i.e. TARGET2-Securities (T2S) and SWIFT[2]. T2S is the common settlement platform for European CSDs that is being rolled out in several migration waves as of 2015. It is covered in the section on securities clearing, settlement and custody. 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, so that SWIFT itself is of systemic importance.

Chart 1 demonstrates that the FMIs, custodians, PSPs and CSPs covered in this report are underpinning financial markets as well as the real economy by providing clearing, settlement, custody and other services to financial intermediaries, and for retail payments, also to the end user. If designed safely and executed properly, they are instrumental in reducing systemic risks and contagion in case of financial crisis.

(1) Continuous Linked Settlement.
(2) Society for Worldwide Interbank Financial Telecommunication.

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



(1) Individual institutions are listed in Table 1.

1.2 FMIs, custodians, PSPs and CSPs subject to oversight and prudential supervision by the Bank

Having illustrated the critical importance of FMIs, such as payment systems, payment schemes, (I)CSDs, CCPs, as well as of custodians, PSPs and CSPs in the functioning of financial markets and payment services, their central role has also been translated in specific regulatory provisions and requirements aiming to ensure the smooth functioning of financial markets, within and across jurisdictions. The international membership of systems and institutions raise legal risks, in particular in case of insolvency of foreign market participants. Legal certainty about the moment when obligations by the FMI or its participants generated in payment, clearing and settlement processes are discharged (i.e. the point of finality of a transaction) is a crucial element in that respect. In the EU, the Settlement Finality Directive[1], applies to all of the payment, clearing and settlement systems in the EU that are designated as being covered by the Directive, as well as all participants in such systems[2]. The Bank does play an active role in the development of regulatory policies and requirements. In the following chapters, specific sections are devoted to changes in the regulatory framework.

Given their central role and systemic importance, the Bank has a broad mandate to conduct oversight and supervision with respect to the systems and institutions covered in this report.

Based on its Organic Law[3], the Bank is responsible for the oversight of payment and securities settlements systems to ensure that they operate properly and to make certain that they are efficient and sound following applicable international standards such as the April 2012 CPMI-IOSCO Principles for Financial Market Infrastructures (PFMIs)[4]. The Bank oversees securities clearing and settlement systems, payment systems and payment schemes, and critical service providers (CSPs).

Since 2011, the Bank has also been designated as micro-prudential supervisory authority for the supervision of individual financial institutions[5]. These include the operators of clearing and settlement systems, such as CCPs and CSDs, as well as custodians and PSPs like PIs and ELMIs. Institutions that have the status of credit institution are, in that capacity, subject to prudential bank supervision. As of November 2014, a substantial part of the related Bank's prudential responsibilities for credit institutions was transferred to the ECB under the Single Supervisory Mechanism (SSM) Regulation[6]. Less significant institutions (LSIs) remain however under the prudential supervision of the Bank as national competent authority.

For new legislation like the 2012 European Market Infrastructure Regulation (EMIR)[7] and the 2014 CSD Regulation (CSDR)[8], the Bank has been assigned as competent supervisory authority. EMIR and its implementing Regulations set out the clearing obligation and the requirements for CCPs established in the EU. CSDR, on the other hand, introduces prudential requirements on the operation of CSDs in the EU, as well as on banking-type ancillary services provided by those CSDs or designated credit institutions.

Table 1 below provides an overview of the systems and institutions supervised or overseen by the Bank. FMIs, custodians, PSPs and CSPs have been classified according to (i) securities clearing, settlement and custody, (ii) payments and (iii) CSPs to the financial infrastructure. These systems and institutions can be further grouped by: (i) type of regulatory role of the Bank (i.e. prudential supervision, oversight or both) and (ii) its international dimension (the Bank as solo authority, international cooperative arrangement with the Bank as lead or in another role). The international scope of the oversight

(1) Directive 98/26/EC of the European Parliament and of the Council of 19 May 1998 on settlement finality in payment and securities settlement systems, OJ. 11 June 1998, L. 166, 45-50 (http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31998L0026&from=EN).

(2) For Belgium, designated systems include the payment systems TARGET2-BE, the Belgian component of TARGET2, and CEC, as well as the securities settlement systems NBB-SSS, Euroclear Bank, Euroclear Belgium.

(3) Art. 8, Law of 22 February 1998 establishing the organic statute of the National Bank of Belgium, *Belgian Official Gazette* 28 March 1998, 9.377.

(4) CPMI-IOSCO (2012), Principles for financial market infrastructures, BIS (http://www.bis.org/publ/cpss101a.pdf).

(5) 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 said Law. The new supervision model was established by the promulgation of the Royal Decree of 3 March 2011 regarding 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.

(6) 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).

(7) 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 (http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012R0648&from=EN).

(8) 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 (http://publications.europa.eu/en/publication-detail/-/publication/e58428b4-2e81-11e4-8c3c-01aa75ed71a1/language-en).

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, Belgian Money Corp, Belmoney Transfert, Gold Commodities Forex, HomeSend, Money International, MoneyTrans Payment Services, Munditransfers, 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, Orange Belgium, 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		

(1) Peer review in Eurosystem/ESCB.

and supervision reflects the international dimension of the FMIs, custodians, PSPs and CSPs, as well as their systemic relevance for other regulatory authorities.

Custodians such as BNYM SA/NV (including its Brussels branch) and PIs and ELMIs are subject to prudential supervision. Following the SSM criteria for identifying systemically relevant credit institutions (SI) within the euro area, BNYM SA/NV is considered as an SI and falls under direct supervision of the SSM.

CCPs and (I)CSDs are subject to both prudential supervision and oversight. While there is no CCP established in Belgium, following the EMIR Regulation, the Bank takes part as a competent authority in 7 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[1]. 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.

As mentioned above, there are three (I)CSDs in Belgium: Euroclear Bank, Euroclear Belgium and NBB-SSS. Only Euroclear Bank has banking status. Unlike BNYM SA/NV, Euroclear Bank has been qualified as a less significant institution (LSI) (i.e. total assets < € 30 billion) and remains under the direct supervision of the Bank as NCA. As the risk profile of an FMI is fundamentally different from a universal deposit-taking bank, prudential requirements for banks (i.e. Basel III, Capital Requirements Directive, etc.) do not always adequately cover the specific operational and financial risks of FMIs. Other internationally agreed standards for CCPs and (I)CSDs are more adequate to cover such risks (i.e. PFMIs). In the EU framework, these principles have been transposed into European legislation (EMIR and CSDR). The owner of Euroclear Bank, Euroclear SA, provides core services to its Group (I)CSDs, including Euroclear Bank and Euroclear Belgium. In order to bring Euroclear SA within the Bank's supervisory scope, it has been designated as an "assimilated settlement institution"[2].

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.

For those institutions subject to both prudential supervision and oversight (i.e. Euroclear (I)CSDs, CCPs, Worldline SA/NV), the Bank aligns its prudential supervision and oversight approach. Synergies between the Bank's prudential supervision and oversight are explained in box 1.

NBB-SSS, the securities settlement system operated by the Bank, is subject to oversight only. Payment systems (TARGET2, CEC, CLS), card schemes (Bancontact, MasterCard Europe) and CSPs such as SWIFT and TARGET2-Securities are also covered by the Bank's oversight.

For the systems and institutions established in Belgium which are systemically relevant in other jurisdictions' financial markets or for the financial industry as a whole, the Bank has established cooperative arrangements with other authorities. This may involve multilateral cooperative arrangements, in which the Bank acts as lead overseer (i.e. SWIFT, Euroclear Bank). Similarly, the Bank takes part in a number of international cooperative arrangements (BNYM SA/NV, TARGET2, TARGET2-Securities and CLS) in which another national authority acts as lead overseer/supervisor.

(1) The FSMA is assigned, together with the Bank, as national competent authority for CCPs under EMIR.
(2) Art. 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.

Box 1 – Oversight and prudential supervision of financial market infrastructures, custodians, payment service providers and critical service providers

The Bank has responsibilities in both oversight and prudential supervision of financial market infrastructures (FMIs), custodians, payment service providers (PSPs), such as payment institutions and electronic money institutions, and

critical service providers (CSPs). 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. At the same time, 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. The main objectives of oversight are the safety and efficiency of FMIs and it pursues these objectives by monitoring existing and planned systems, assessing them and, where necessary, inducing change. The oversight of FMIs has now come to be 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 and focuses on the safe and efficient functioning of payment, clearing and settlement services 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 CSP of systemic importance. SWIFT is therefore subject to a (cooperative) central bank oversight arrangement.

Since the adoption of the 'twin peaks' supervision model in April 2011, the Bank is also responsible for prudential supervision, including of the regulated institutions operating some of these FMIs. Since 2013, the responsibility for prudential supervision of credit institutions in the euro area has been transferred to the Single Supervisory Mechanism (SSM) led by the ECB. Significant institutions, such as Bank of New York Mellon SA/NV are directly supervised by the SSM. For less-significant institutions, the Bank remains the 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 focusses on the sound functioning of the settlement system (by assessing compliance with oversight standards), the prudential supervision focusses on the financial soundness of the operator (by assessing compliance with banking regulations).

Another distinction relates to the topics covered by oversight and prudential supervision. 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 CSP. Typical areas oversight is focussing on cover the functioning of the system and how its organisation minimises or avoids risks. Examples thereof include settlement finality rules reducing risks linked to the insolvency of participants, delivery versus payment or payment versus payment mechanisms eliminating principal risks and stringent requirements on business continuity plans. 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, including prudential supervised operators of FMIs, 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 2012 Principles for FMIs (PFMIs) of the BIS Committee on Payments and Market Infrastructures (CPMI) and the International Organisation of Securities Commissions (IOSCO) cover payment systems, securities settlement systems, central securities depositories (CSDs), central counterparties (CCPs) and

Trade Repositories. For the implementation of these principles, further clarity and granularity is provided by relevant guidelines such as the CPMI-IOSCO Guidance on cyber resilience for FMIs or forthcoming guidance on resilience and recovery of CCPs. In addition, the CPMI also published, for example, an analytical framework for distributed ledger technology in payment, clearing and settlement. If FMIs have a banking status, or for other types of institutions such as custodians, prudential supervision is based on applicable banking regulation (Capital Requirements Directive, Bank Recovery and Resolution Directive, etc.).

Finally, also the tools to conduct oversight and prudential supervision differ. Oversight is generally based on principles and guidelines designed in international fora (Eurosystem, CPMI, CPMI-IOSCO), pressing FMIs and CSPs into adhering these 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 translated in EU directives and local laws ("hard law" approach). Over time, central bank oversight has become more formal, following the increasing role of the private sector in providing payment and settlement systems, as well as the growing criticality of these systems' proper functioning. In some cases, oversight also evolves to a hard law approach as illustrated, for example, by the new Belgian law on systemically relevant processors for retail payment instruments.

In order to pool expertise and reinforce the synergies between the oversight function and that of prudential supervision on FMIs, custodians, PSPs and CSPs, these two functions have been integrated into the same department within the Bank.

The PFMIs, which also cover responsibilities of supervisory and other authorities, provide that relevant authorities should cooperate with each other, both domestically and internationally, in promoting the safety and efficiency of FMIs. Domestically, the Bank cooperates with the FSMA which has responsibilities in the supervision of financial markets with regard to conduct of business rules. The implementation of the PFMIs, including the responsibilities of authorities, is being monitored by CPMI and IOSCO[1]. With regard to PFMI Responsibility E (i.e. cooperation with other relevant authorities), the Bank has been assessed (November 2015) as "broadly observed" for Euroclear Bank[2]. The fact that full compliance was not reached was due to (i) a lack of formalisation of the cooperation modalities with the Luxembourg authorities that was to be extended to a broader scope than the link (the so-called Bridge) between Euroclear Bank and Clearstream Banking Luxembourg, (ii) the fact that not all relevant foreign authorities are formally consulted and (iii) not all relevant central banks of issue are formally invited to provide views during assessments. In response to these recommendations, the Bank started in 2016 a formal multilateral cooperation with the Federal Reserve, Bank of England, Bank of Japan and the European Central Bank (as observer), which are the central banks of issue of the major settlement currencies in Euroclear Bank. Their views of Euroclear Bank's payment and settlement arrangements and its related liquidity risk management procedures are now being considered by the Bank in the context of assessing Euroclear Bank's observance of the PFMIs. As Euroclear Bank has a wide international range of activities, 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. The extension of the cooperation with the Luxembourg authorities (with the European Central Bank as observer), focusing on the implementation of the PFMIs by both ICSDs, is expected to enter into force on short notice.

(1) Following the publication of the PFMIs, the CPMI and IOSCO agreed to monitor their implementation in 28 jurisdictions with authorities that are members of the Financial Stability Board (FSB) and/or the CPMI and/or the IOSCO. This is done through implementation monitoring assessments which are being conducted at three levels: a Level 1 (L1) assessment of the status of the implementation process, a Level 2 (L2) assessment of the completeness of the implemented framework and its consistency with the PFMIs, and a Level 3 (L3) assessment of the consistency in outcomes of such frameworks.

(2) CPMI-IOSCO (2015), *Assessment and review of application of Responsibilities for authorities*, BIS (http://www.bis.org/cpmi/publ/d139.pdf).

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 are 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 submit to supervision. 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 regulation made central clearing for standardised OTC derivatives mandatory. While there is no CCP established in Belgium, the Bank takes part in seven EMIR CCP regulatory colleges as supervisor of (I)CSDs to which the CCP is linked or as supervisor of Belgian Clearing Members providing large contributions to the CCP's default fund. (I)CSDs, responsible for the last stage in the post-trade chain, are dealt with in Section 2.2. Among the (I)CSDs hosted by the country, Euroclear Bank and Euroclear Belgium are subject to both prudential supervision and oversight, while NBB-SSS is subject to oversight only. The only (I)CSD with banking status is Euroclear Bank. It falls under the prudential authority of the European Central Bank (ECB). However, as Euroclear Bank has been qualified as a less significant institution (LSI) under the SSM, it remains under the direct prudential supervision of the Bank as national competent authority. 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. BNYM SA/NV is supervised by the ECB under the framework of the SSM as a significant credit institution (SI).

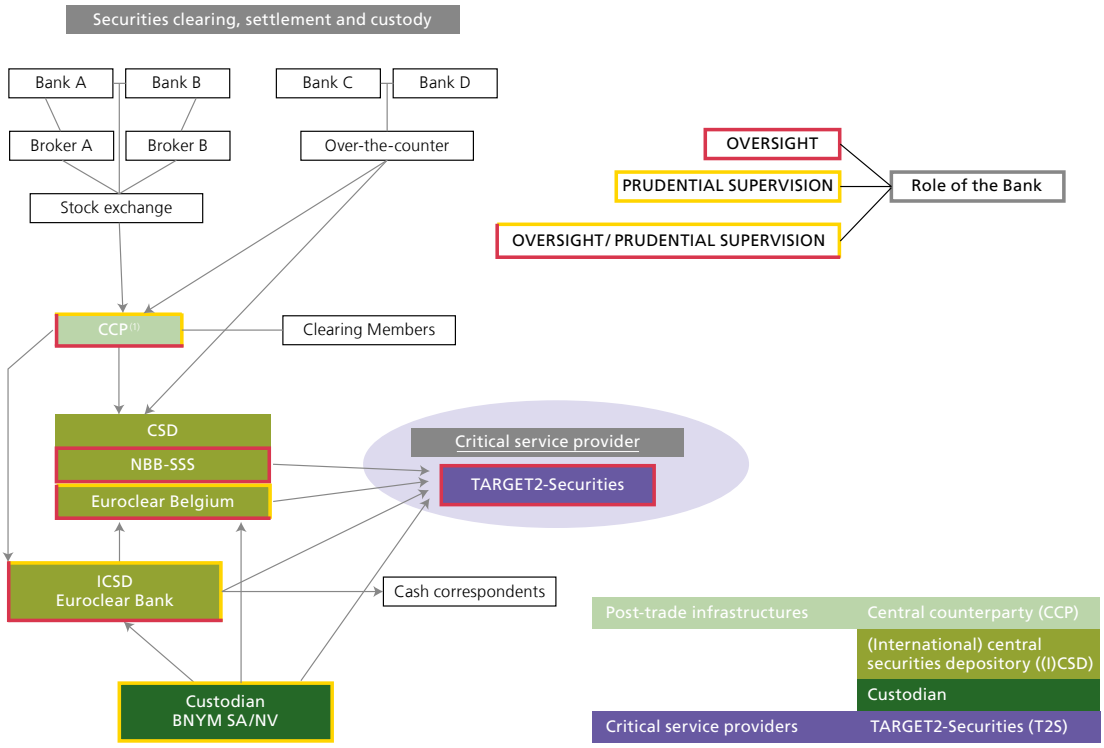
2.1 CCPs

CHANGES IN REGULATORY FRAMEWORK

In 2009, the G20 leaders took the initiative to make the over-the-counter (OTC)[1] derivatives markets safer and more transparent. They decided that all standardised OTC derivatives contracts should be cleared through a CCP with the aim to enhance financial stability. As a result, CCPs have become increasingly critical components of the financial system in recent years. A CCP interposes itself between the counterparties, becoming the seller to the buyer and the buyer to the seller, and manages the outstanding risk on the contracts, mainly via collateralisation. The original counterparts to the trade now have a risk on the CCP, and no longer on each other. In order to fully reap the benefits of CCPs, they should be subject to strong regulation and supervision. In April 2015, under the guidance of the Financial Stability Board (FSB), the Basle Committee on Banking Supervision (BCBS), CPMI and IOSCO agreed a work plan to coordinate their policy work to enhance the resilience, recovery planning and resolvability of CCPs. The work plan focuses on CCPs that are systemic across multiple jurisdictions.

(1) An over-the-counter trade is a trade concluded via a dealer network, as opposed to on a centralised exchange.

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



(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).

At international level, two reports were issued subsequently. Firstly, in August 2016, an FSB update report on the work undertaken to address risks posed by CCPs was published. The report refers to the work of a dedicated working group on the interdependencies between CCPs and their clearing members, users and other stakeholders such as liquidity providers, and on the (dis)incentives of other regulations to promote central clearing. The main focus was nonetheless on aspects of CCP resilience (i.e. the safeguards that make a CCP sound and prevent its failure), CCP recovery (i.e. the pre-agreed measures to refund or recapitalise a CCP in case it would encounter major financial and/or operational difficulties, to keep it operating) and CCP resolution (whereby the authorities step in, either to save the CCP although not with public money, or to orderly wind it down)[1].

Secondly, the FSB published in early February 2017 a consultative report with draft Guidance on Central Counterparty Resolution and Resolution Planning, setting out proposals for effective resolution strategies. The report seeks to complement the FSB's Key Attributes of Effective Resolution Regimes for Financial Institutions (Key Attributes) and implementation guidance on FMI resolution. The Key Attributes state the objectives of FMI resolution and a range of powers and tools that should be made available to resolution authorities to resolve a failing FMI. The guidance sets out the tools to be used for the effective resolution of CCPs, aiming to assist resolution authorities with developing credible resolution strategies and plans. It covers timing of entry into resolution, adequacy of financial resources, tools for returning to a matched book and allocating default and non-default losses, application of the "no creditor worse off" safeguard[1], treatment of the CCP's equity in resolution, and cross-border cooperation and effectiveness of resolution actions.

(1) Swerts, Q., and Van Cauwenberge, S. (2016), *CCP resilience and recovery, Impact for the CCP users*, NBB Financial Stability Report, 187-202 (https://www.nbb.be/doc/ts/publications/fsr/fsr_2016.pdf).

The CPMI and IOSCO intend to publish in Q2 2017 a report with additional guidance on the resilience of central counterparties (CCPs). The guidance aims to provide more granularity to the standards set out in the PFMIs. The proposed guidance focuses on CCP governance, credit and liquidity stress testing, margin, a CCP's contribution of its financial resources to losses, and its coverage of credit and liquidity resource requirements. The report also recalls the relevance of having a credible recovery plan in place.

In the EU, the 2012 EMIR Regulation and its implementing Regulations set out the clearing obligation and the requirements for CCPs established in the EU Member States. In 2016, the clearing obligation entered into force in the EU for standardised Interest Rate Swap (IRS) contracts in the most relevant currencies, and for indexed Credit Default Swaps (CDS)[2]. The obligation will be phased in based on a dedicated calendar, whereby the bigger counterparties have to cope with the obligation first. As scheduled, the European Commission started its consultation on the review of EMIR mid-2015, and published its EMIR review report in November 2016[3]. A legislative proposal is expected Q2 2017. Overall, no big change to the EMIR framework is expected, with the main focus on fine-tuning some requirements or increasing the efficiency. Furthermore, in November 2016, a more detailed proposal from the Commission set out the CCP recovery and resolution frameworks, based on the international work.

BUSINESS ACTIVITY

Chart 3 shows the value of amounts cleared over 2015 in the main EU CCPs, broken down into four broad product categories cleared, i.e. cash market instruments, non-OTC and OTC derivatives, and repo transactions. Most CCPs are multi-product CCPs, although not to a comparable extent. A CCP is by definition systemically important: it concentrates credit, liquidity and operational risks as it becomes a counterparty to every buyer and seller. Nonetheless, four EU CCPs – Eurex Clearing AG (DE), the sister CCPs LCH.Clearnet SA (FR) and LCH.Clearnet Ltd (UK), and ICE Clear Europe (UK) – can be said to be very important from a financial stability perspective, on the basis of both their sheer activity level (shown in chart 3) and the risks they manage (as shown hereafter, Table 5).

There is currently no CCP established in Belgium. However, CCPs are relevant for Belgian financial markets, clearing members and CSDs. The four most important CCPs from an EU perspective are also the most relevant CCPs for Belgium given their role in clearing the Belgian cash and derivatives on exchange markets[4], OTC derivatives products and repos. Other relevant aspects include the number of Belgian clearing members and the Belgian CSDs the CCP settles in[5].

The Euronext Brussels exchange markets are cleared by the French central counterparty LCH.Clearnet SA. Over 2016, the Euronext Brussels cash market trade volumes cleared by LCH.Clearnet SA amounted to € 120 billion. The notional values of futures traded comprised € 2.5 trillion over the year and € 617 billion for option products.

A number of EU CCPs clear OTC derivatives products that are, as opposed to listed derivatives, not standardly cleared by a CCP. Nowadays, the main OTC derivative product categories cleared by CCPs are interest rate and credit default products. In its mid-2016 progress report the FSB indicates that 60 % of the OTC interest rate derivatives products can be CCP cleared, compared to less than 30 % for credit derivatives[6]. As can be seen from the outstanding amounts at end-2016 – see table 2 – clearing is quite concentrated. The London-based CCP LCH.Clearnet Ltd estimates that its SwapClear service cleared 50 % of all OTC IRSs worldwide, and even 95 % of the contracts cleared by a CCP. Around 40 % of the IRSs cleared by LCH.Clearnet Ltd are denominated in euro. At the end of 2016, the notional amount outstanding of cleared IRSs amounted to € 240 trillion. The main EU CCP clearing CDSs is ICE Clear Europe, also

(1) The "no-creditor-worse-off" principle implies that no creditor will receive less in economic terms than what it would have received under regular insolvency proceedings of the CCP, without the resolution authority intervening.

(2) An IRS is a financial derivative instrument in which two parties agree to exchange interest rate cash flows, thereby hedging or taking a position in an interest rate. With a CDS, counterparty credit risk is hedged or taken. Only the most liquid IRSs or CDSs are subject to a clearing obligation. ESMA holds a "Public register for the clearing obligation under EMIR" on its website, available via https://www.esma.europa.eu/regulation/post-trading/otc-derivatives-and-clearing-obligation.

(3) The Commission's EMIR review report is available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0857&from=EN.

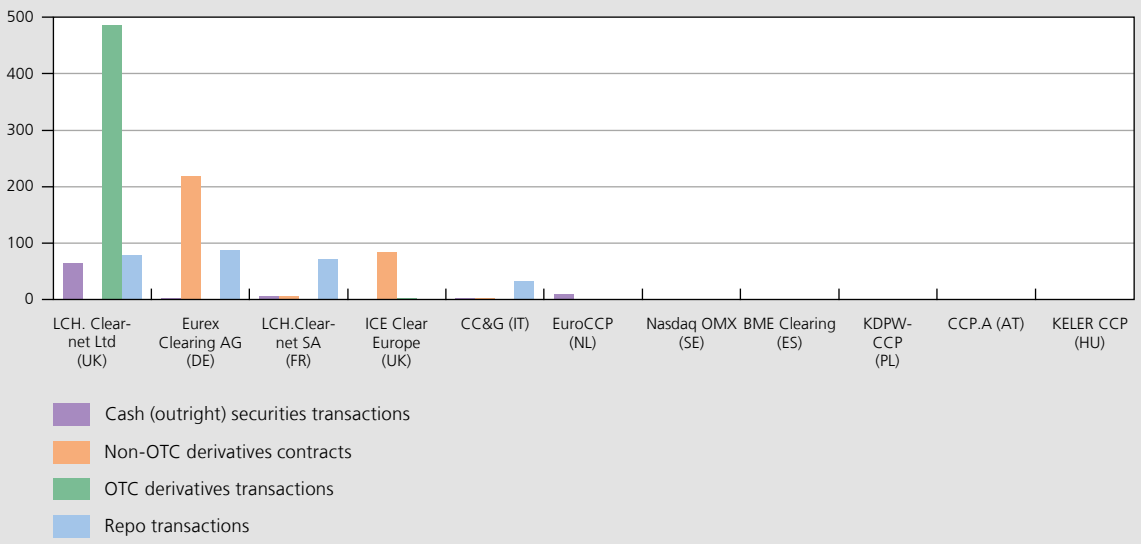
(4) On exchange is a term to indicate that a trade is taking place directly on an order book.

(5) For these aspects, see hereafter, this chapter, prudential and oversight approach and table 4.

(6) OTC Derivatives Market Reforms: Eleventh FSB Progress Report on Implementation (26 August 2016).

CHART 3 VALUE OF AMOUNTS CLEARED IN THE MAIN EU CCPs

(2015 yearly total, in € trillion)[1]



Source: ECB Blue Book, 2015 data.
(1) For derivative trades, the notional amounts cleared are represented.

established in London. Its notional outstanding value of CDSs amounted to about € 1.5 trillion at end-2016, compared with € 56 billion for the Paris-based LCH.Clearnet SA.

As regards secured euro lending, mainly repo trades, according to the ECB's 2015 Euro Money Market Survey[1], around 70 % of the overall EU market turnover was CCP-cleared. The CCP clearing of repo trades is also heavily concentrated, with nearly equal parts cleared by the main EU CCP, as can be seen from table 3. According to the semi-annual International Capital Markets Association (ICMA) European Repo Market Survey, the total value of repo contracts (over all currencies) outstanding in the EU was almost € 5.7 trillion by mid-December 2016.

TABLE 2 OVER-THE-COUNTER DERIVATIVES CLEARING VALUES IN MAIN EU OTC DERIVATIVES CCPs

(notional amounts outstanding end 2016, in € billion)

EU derivatives CCP	Interest Rate Swaps (IRS) and Forward Rate Agreements (FRA)	Credit Default Swaps (CDS)
LCH.Clearnet Ltd (UK)	240 193	n.
ICE Clear Europe (UK)	n.	1 467
Eurex Clearing AG (DE)	945	n.
LCH.Clearnet SA (FR)	n.	56

Sources: CCP websites.

(1) https://www.ecb.europa.eu/stats/financial_markets_and_interest_rates/money_market/html/index.en.html.

TABLE 3 REPO CLEARING VALUES IN MAIN EU CCPs
(2016 yearly total, in € billion)

CCP	Values[1]
LCH.Clearnet Ltd (UK)	74 275
LCH.Clearnet SA (FR)	67 534
Eurex Clearing AG (DE)	65 293
ICE Clear Europe (UK)	n.

Sources: CCP websites.
(1) Trade (gross) values are double counted due to the CCP interposition.

In mid-2016, the Deutsche Börse Group and the London Stock Exchange (LSE) Group announced their intention to merge. This proposed consolidation was to a considerable extent driven by the CCP activities of the groups. The sister CCPs LCH.Clearnet SA and LCH.Clearnet Ltd, and the Italian CCP CC&G are LSE Group companies, while Eurex Clearing is the CCP of the Deutsche Börse Group. The merger was expected to allow CCP customers to clear more trades and hold bigger positions while providing a smaller amount of collateral, which would also further concentrate or interconnect the risks to be managed by the (combined) CCPs, potentially impacting financial stability (this aspect is set out in the article on "Concentration risks in financial market infrastructures – the specific case of CCPs"). At the end of March 2017, however, the European Commission's Directorate-General for Competition blocked the merger.

PRUDENTIAL & OVERSIGHT APPROACH

From a microprudential perspective, the most relevant financial risks faced by a CCP are counterparty credit risk and liquidity risk. Counterparty credit risk refers to the risk that a counterparty will be unable to fully meet its obligations, mainly following a clearing member (CM) default occurring 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, 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 to have adequate resources to cover the loss or to raise the liquidity needed in time. In other words, the CCP has to comply at all times with the so-called CPMI-IOSCO "cover 2" principle.

In April 2016, the European Securities and Markets Authority (ESMA) published the results of its first supervisory stress test for EU CCPs. The test focused solely on the counterparty credit risk which CCPs would face as a result of multiple CM 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-2 EU-wide CM groups under both historical and hypothetical market stress scenarios. Under more severe stress scenarios – and especially the case assuming the default of the top-2 CMs of each EU CCP leading to more than 25 CM defaulting EU-wide – CCPs faced only small total (i.e. across all CCPs) residual uncovered losses. Wherever it appeared that a CCP did not always use a severe enough scenario, this was notified to its national competent authority for supervisory follow-up[1]. The second ESMA EU-wide CCP stress test, scheduled for 2017, will also include a liquidity stress-testing part. This is not a mere add-on feature, but testing of an important CCP risk management challenge. It should not be forgotten that the 2008 crisis appeared as a liquidity crisis.

As of end-2016, the Bank was participating in seven CCP supervisory colleges, as listed in table 4. Its participation is based either on its capacity as supervisor of a CSD that the CCP settles in, or as supervisor of CMs of the CCP that contribute the most to the default fund per country.

(1) The report on the EU-wide ESMA 2015 CCP stress test 2015 is available at: https://www.esma.europa.eu/sites/default/files/library/2016-658_ccp_stress_test_report_2015.pdf. Details of the announced ESMA 2017 CCP stress test are available at https://www.esma.europa.eu/press-news/esma-news/esma-announces-details-2017-ccp-stress-test.

TABLE 4 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	2 Belfius Bank; BNP Paribas Fortis		X (EB)
LCH Clearnet SA (FR)	Euronext cash and derivatives trades (including Euronext Brussels)	7 Banque Degroof Petercam; Belfius Bank; BNP Paribas Fortis; Delen Private Bank; Dierickx Leys & Cie Effectenbank; 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) The Bank participated until November 2016 in the college of the national Polish KDPW_CCP, but no longer does so. Under European rules, the CCP college participation is yearly reassessed based on the EMIR Art. 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 is eventually a foreign entity of the group it belongs to.

(3) EB: Euroclear Bank ICSD, EBE: Euroclear Belgium CSD, NBB-SSS: securities settlement system operated by the Bank.

A rough indication of how big a CCP is, or how much "risk" it manages, consists in looking at the overall initial margin[1] amounts it receives – across all of its CMs – and at its default fund[2] resources. Although the products cleared and the specific risk management methods used by the CCPs do differ, the overall structure and requirements for initial margin and default fund calculations are prescribed by the EMIR Regulation. The data in table 5 are thus to a certain extent comparable across CCPs. They relate to the initial margins and default fund of the main EU CCPs or CCPs where the NBB participates in the supervisory college.

(1) Initial margin is the collateral that the clearing member provides to the CCP to open or maintain a position, and that covers the potential future price movements of a contract or portfolio over the so-called 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.

(2) 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. The size of the default fund should allow a CCP to withstand the simultaneous default of its two biggest clearing members, under extreme but plausible market conditions

TABLE 5 PRE-FUNDED RESOURCES AVAILABLE TO SELECTED EU CCPs

(in € billion)

CCP	Initial margins collected[2]	Default fund resources[3]
LCH.Clearnet Ltd[1] (UK)	77	5.4
Eurex Clearing AG[1] (DE)	47	3.6
ICE Clear Europe[1] (UK)	42	2.5
LCH.Clearnet SA[1] (FR)	23	3.2
CC&G[1] (IT)	12	4.9
Nasdaq OMX (SE)	5	0.4
BME Clearing (ES)	4	0.2
EuroCCP[1] (NL)	2	0.2
KDPW_CCP (PL)	0.3	0.1
Keler CCP[1] (HU)	0.05	0.02
CCP.A (AT)	0.03	0.02

Sources: CPMI-IOSCO quantitative disclosure framework (tables 4.1 and 6.1), Q3 2016, as disclosed by the CCP.

(1) The Bank participates in the supervisory college of the CCP.

(2) Initial margins are summed over all clearing members of the CCP. In case of a clearing member default the CCP will only use the initial margin of the defaulter, not the initial margin of the surviving clearing members.

(3) Where a CCP has more than one default fund, the sum of the sizes of all default funds is taken. In case of a clearing member default, the CCP can use the whole default fund if needed.

SUPERVISORY PRIORITIES IN 2017

Priorities for the ongoing supervision of EU CCPs are set by the national competent authority, taking into account the college members' demands. The most relevant priorities for the EU CCPs in general are set out below.

Pending EU legislation on CCP resolution, and given the FSB initiatives, national competent authorities are starting to establish cross-border crisis management groups for CCP resolution and looking on how to implement the CCP resolution plan. As a corollary, and based on the CPMI-IOSCO guidance on FMI recovery – CCPs are enhancing their recovery rules and the way stakeholders, including the CMs, share in the losses. Furthermore, a continuing priority remains the CCP's operational (and specifically its cyber) risk management. Also, ESMA – in its role of responsible authority for harmonising the supervisory practices across the EU CCPs – has issued a report containing recommendations for best practices regarding margin and collateral requirements, including recommendations on portfolio margining[1]. National competent authorities are expected to follow this up. Finally, an ongoing supervisory activity is the 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 authorised by its national competent authority that has to take into account the opinion of the CCP's supervisory college. For instance, at the end of 2016, the London CCP LCH.Clearnet Ltd announced its plan to offer a clearing service for OTC FX options, for which an authorisation and thus a college opinion is required.

(1) With portfolio margining, the margin requirements are calculated on the basis of the overall risk of the portfolio of a given product class. Portfolio margining results in lower margin requirements on hedged positions. See also ESMA (2016), Peer Review under EMIR Art. 21 – Supervisory activities on CCPs' Margin and Collateral requirements (https://www.esma.europa.eu/press-news/esma-news/esma-identifies-areas-improvement-in-eu-ccp-supervision).

2.2 (I)CSDs

CHANGES IN REGULATORY FRAMEWORK

The implementation of the CSD Regulation (CSDR)[1] will be a regulatory milestone for the (I)CSD sector in the EU. It will usher in a uniform set of rules for the supervision of (I)CSDs. The final draft regulatory technical standards were adopted by the European Commission in November 2016 and have become effective as from end-March 2017[2]. These include 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. 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[3] or to designate for that purpose one or more credit institutions. If two (I)CSDs are linked with each other based on mutual operational procedures, any such interoperable link needs to be licensed as well.

The authorisation of an (I)CSD is the responsibility of its competent authority; i.e. the Bank in the case of Belgian (I)CSDs. Euroclear Belgium only needs a (I)CSD licence. Euroclear Bank needs to obtain an authorisation to provide both (I)CSD and banking-type ancillary services. The interoperable link between Euroclear Bank and Clearstream Luxembourg (the Bridge) needs to be authorised as well. The rules for authorisation and supervision of (I)CSDs under CSDR are not applicable to the members of the ESCB, Member States' national bodies performing similar functions or other public bodies[4]. This implies that NBB-SSS, the CSD operated by the Bank, does not need to obtain a CSDR licence and is not subject to supervision. However, from a legal perspective, NBB-SSS also needs to be compliant with the CSDR no later than one year after its related regulatory technical standards entered into force.

The CSDR will have an impact at different levels, either direct or indirect, on market participants using the (I)CSDs or on other stakeholders such as issuers. Most CSDR requirements will be effective as soon as an (I)CSD has obtained its CSDR licence; i.e. their impact will therefore materialise in the short term. Other requirements will only be effective at a later stage. The main areas with impacts on participants and issuers are summarised below.

Participants of (I)CSDs are directly impacted in various domains. A first area relates to reconciliation practices. Under the CSDR and with the aim of limiting potential contagion effects, (I)CSDs are obliged to suspend securities settlement when reconciliation reveals an undue creation or deletion of securities that cannot be solved by the (I)CSDs by the end of the next day. In that framework, participants have to reconcile their records with the information received by the (I)CSDs on a daily basis and will need to provide the (I)CSD with all information deemed necessary to ensure the integrity of the issue and to solve any reconciliation breaks. Another area is about account segregation. The CSDR requires (I)CSDs to allow its participants to segregate the securities they hold on behalf of underlying clients either via omnibus or individual client segregation. A third area with a potential impact on participants relates to internal settlement on (I)CSDs' participants own books, outside of securities settlement systems. Depending on the size of the internalised settlement volumes, specific reporting by the participants of the (I)CSD directly to the relevant competent authorities of the (I)CSD is necessary.

The CSDR requirements also contain some specific obligations for issuers. In the framework of (I)CSDs' record-keeping requirements under the CSDR, the use of a Legal Entity Identifier (LEI) – a unique character code to identify legal entities – is aimed to contribute to a harmonisation of data collection and reporting among the EU. As not all issuers and participants have an LEI today, they will have to apply for one in the future.

There will also be immediate indirect effects as soon as the new Regulation enters into force. As (I)CSDs providing banking ancillary services need to cover any credit use of participants, intraday or end-of-day, with collateral or other equivalent financial resources, participants will have to provide high-quality liquid assets in accordance with the collateral categories as defined under the CSDR.

(1) Regulation (EU) N. 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 (http://publications.europa.eu/en/publication-detail/-/publication/e58428b4-2e81-11e4-8c3c-01aa75ed71a1/language-en).

(2) Except for the regulatory technical standards relating to settlement discipline.

(3) 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).

(4) Art. 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.

Two years after the relevant regulatory technical standards for settlement discipline will have entered into force, rules will become applicable introducing cash penalties and mandatory buy-ins for settlement failures. If a settlement instruction fails to settle by the intended settlement date, participants will face a cash penalty that will be collected and redistributed to the impacted counterparts by the (I)CSD. Should the security not be delivered with a certain timeframe following the intended settlement date[1], a mandatory buy-in process is to be triggered.

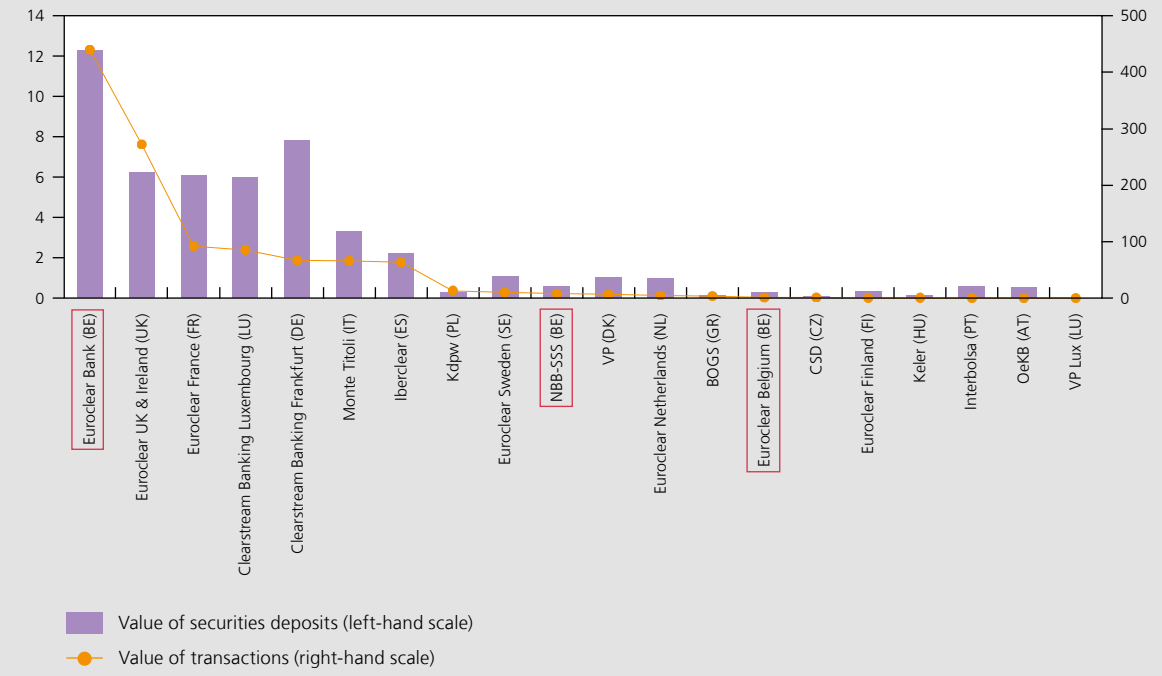
Apart from the CSDR, other regulatory guidelines have been developed in the area of cyber resilience and recovery plans. In June 2016, CPMI and IOSCO jointly published guidance on cyber resilience for FMIs, providing additional details to the PFMIs on how FMIs can enhance their cyber resilience capabilities to limit the increasing risks that cyber threats pose for them, and thus for financial stability in general. In August 2016, the NBB made public[2] 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[3]. The Communication provides information regarding the Bank's expectations for the recovery plan in accordance with the requirements set by international bodies, including the guidelines offset out in the CPMI-IOSCO report on recovery of FMIs.

BUSINESS ACTIVITY

The activities of the (I)CSDs established in Belgium (i.e. NBB-SSS, Euroclear Belgium, Euroclear Bank) in terms of securities deposits and settlement turnover take a prominent position in the European (I)CSD landscape. Chart 4 gives an overview of the top-20 (I)CSDs which are ranked based on 2015 data for total activity in value terms of securities deposits and

(1) This period depends on the asset type and liquidity of the relevant financial instrument.
(2) Communication NBB_2016_37/*Recovery plans – Specific guidelines for Belgian Central Securities Depositories (CSD) and institutions supporting them*, 3 August 2016 (https://www.nbb.be/en/articles/communication-nbb201637-recovery-plans-specific-guidelines-belgian-central-securities).
(3) 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.

CHART 4 SIZE OF (I)CSD SECTOR IN EUROPE IN TERMS OF SECURITIES DEPOSITS AND SETTLEMENT TURNOVER (2015 YEARLY TOTAL, IN € TRILLION)[1]



Source: ECB (Blue Book).
(1) Ranking based on total activity in value terms of securities deposits and settlement turnover.

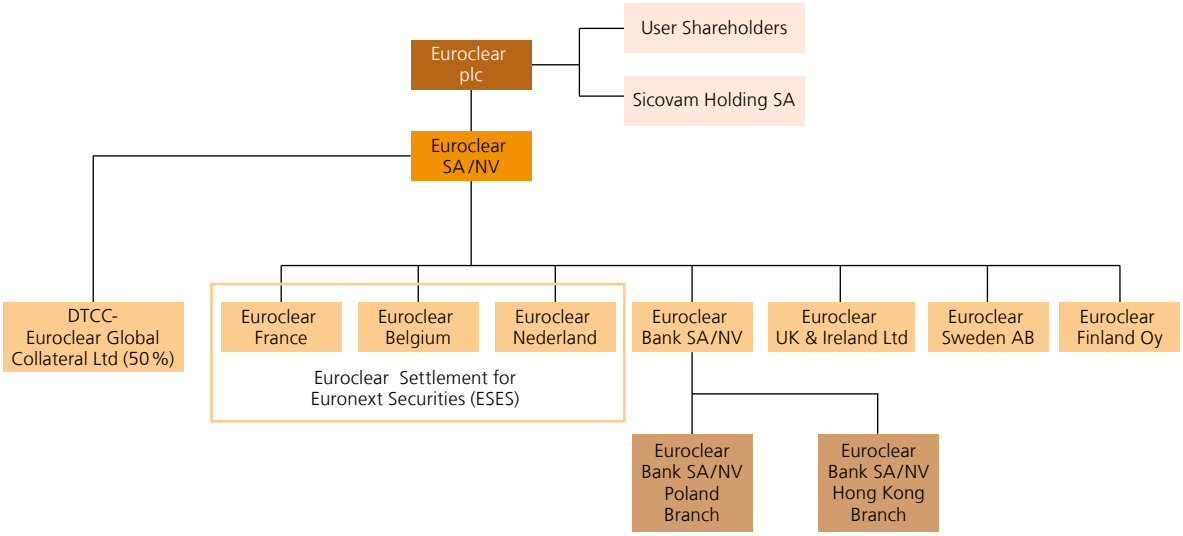
settlement turnover. Belgian (I)CSDs account for about 25 % of total securities deposits in value reported to be held in EU (I)CSDs. In terms of settlement turnover in value, Belgian (I)CSDs represent about 40 % of total aggregate turnover of all EU (I)CSDs. The relevance of the Belgian (I)CSDs for the mobilisation of collateral, including for monetary policy purposes, is also highlighted below.

Euroclear Bank

As shown in chart 5 below, Euroclear Bank is owned by Euroclear SA/NV (ESA). 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 and Hong Kong. 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. Sicovam Holding SA, a holding company that brings together the former shareholders of Euroclear France, is the single largest shareholder of Euroclear plc. Several of the shareholders of Sicovam Holding are also users of the Euroclear system. Euroclear Belgium, Euroclear France and Euroclear Nederland are operating a common settlement platform; i.e. the Euroclear Settlement of Euronext-zone Securities system (ESES) (see section on Euroclear Belgium). Apart from being owned by the users of its services, the Euroclear Group is also governed by its users via their representation on the (Euroclear plc and Euroclear SA) 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 (see below on the role of Belgian (I)CSDs in the mobilisation of collateral).

CHART 5 EUROCLEAR GROUP CORPORATE STRUCTURE
(simplified diagram)

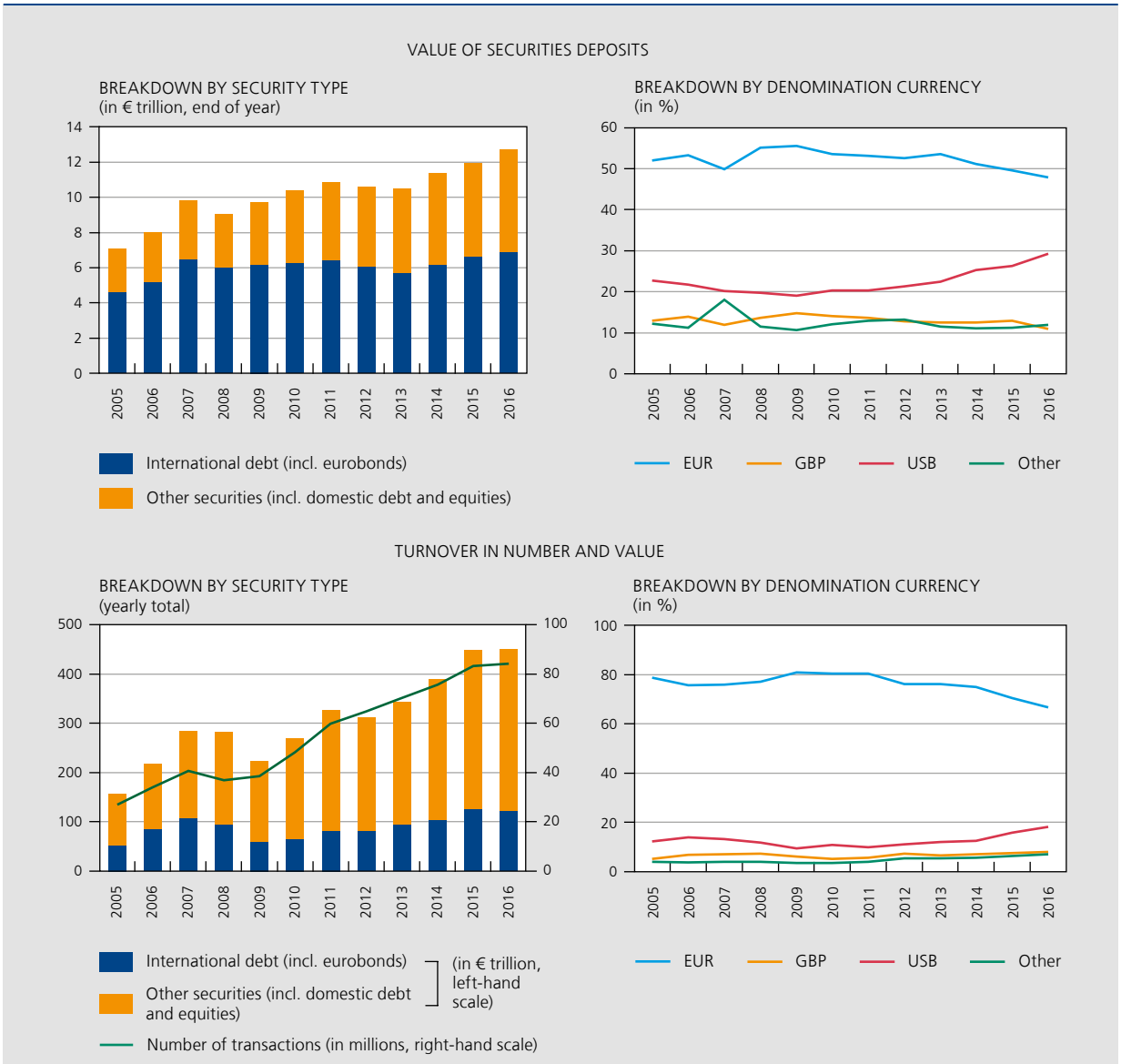


Euroclear Bank is an issuer CSD for international securities, but it also acts as an investor ICSD through its connections with more than 45 securities markets worldwide. Thanks to these links, participants can hold and settle domestic securities issued in all those markets, typically government bonds and other fixed-income securities. Euroclear Bank is rated AA+ by Fitch and AA by S&P[1].

At the end of 2016, the value of securities deposits held on Euroclear Bank's books on behalf of its participants (chart 6, top panel) has grown by 2.5 % to nearly € 12.7 trillion equivalent compared to previous year. A small majority of securities deposits are in international bonds, such as Eurobonds, for which issuers can choose the currency or country of issue. Both Euroclear Bank and Clearstream Banking Luxembourg are the "issuer ICSD" or the primary places of

(1) Euroclear Bank has been qualified, based on the related EBA guidelines, as Other Systemically Important Institution (O-SII). Based on relevant authorities' assessment of systemic risk, higher loss absorbency requirements are set on O-SIIs and with the obligation to maintain a CET1 capital buffer of up to 2 % of the total risk exposure amount. For Euroclear Bank, the final O-SII buffer has been set at 0.75 % by the Bank. The list of O-SII notified to the EBA can be consulted at http://www.eba.europa.eu/risk-analysis-and-data/other-systemically-important-institutions-o-siis-/2016.

CHART 6 SECURITIES DEPOSITS AND SETTLEMENT TURNOVER IN EUROCLEAR BANK



Source: Euroclear.

deposit for this type of securities, unlike for domestic securities where only one CSD acts as the primary place of deposit. More than 60 % of total issuance in Eurobonds is held in Euroclear Bank [1]. Securities held by participants on Euroclear Bank's books can be denominated in more than 50 currencies. After EUR (close to 48 %), USD is the main denomination currency (29 %), followed by GBP (11 %).

Regarding settlement turnover (chart 6, bottom panel), the number of transactions settled in Euroclear Bank amounted to 84.1 million in 2016, a slight increase of 1.0 % compared to 83.3 million in 2015. In value terms, this represents € 451.7 trillion for 2016 as a whole (+2.1 % from € 442.6 trillion in 2015). On average, Euroclear Bank processes more than 326 000 transactions daily with a total value of € 1.75 trillion. A historical peak day (in terms of settlement turnover in value) was recorded in June 2016, just before the Brexit referendum, with more than € 2.13 trillion of transaction value settled in Euroclear Bank. In terms of settlement turnover per security type, compared to securities deposits, international debt accounts for about 27 % of settlement turnover while the bulk is composed of other types of securities such as domestic debt and, to a lesser extent, equities or exchange-traded funds (ETFs). The relative share of the USD has been steadily growing throughout the years, at the expense of EUR activity. In 2016, about 66.7 % of settlement turnover, free of payment and against payment transactions, was denominated in EUR, its lowest level since 2005. USD follows with 18.1 % and GBP with 8.1 %.

NBB-SSS

NBB-SSS, the securities settlement system operated by the Bank, acts as the register ("issuer CSD") for both Belgian public and private sector fixed-income debt. Public sector debt includes securities issued by the Belgian federal government and by regional or local governments. Private sector debt registered in NBB-SSS can be issued by corporates, credit institutions or other entities.

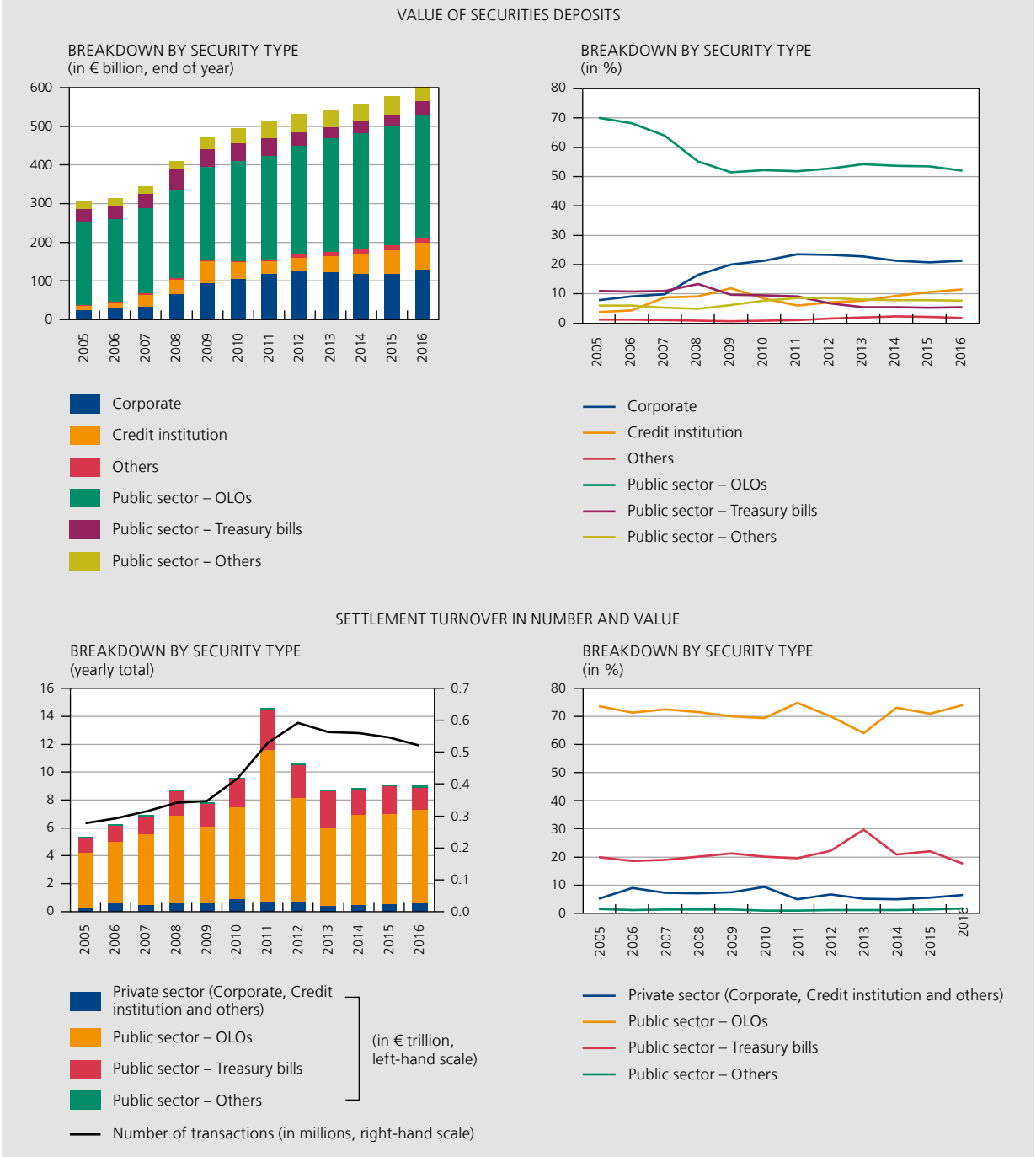
At the end of 2016, total outstanding securities deposits in value (chart 7, top panel) amounted to € 612.5 billion, a 6.4 % increase compared to 2015 (€ 575.4 billion). Total public sector debt securities (OLOs, Treasury bills and others) represent about 65 % of total securities deposits, their lowest share so far. OLOs represent the largest category of securities in NBB-SSS; i.e. 52 % of total securities deposits or close to 80 % of total public sector debt.

In terms of securities settlement turnover (chart 7, bottom panel), the number of transactions settled in NBB-SSS, both new issues and secondary market transactions, dropped from 546 712 in 2015 to 521 729 in 2016 (–4.6 %); a daily average of 2 045 transactions. Settlement turnover in value terms reached € 8.97 trillion or about € 35.2 billion per day on average. This is a slight decrease from € 9.04 trillion recorded in the previous year. About 75 % of settlement turnover in value in 2016 was in OLOs, followed by Treasury bills (18 %). The share of private debt remains marginal compared to public debt. Settlement turnover of private sector debt in value has increased but still only accounts for 6.5 %.

At the end of March 2016, NBB-SSS migrated to the TARGET2-Securities (T2S) platform as part of the second T2S migration wave (see also box 2 on T2S). NBB-SSS adopted a two-step migration with a first phase of T2S functionalities already being implemented in February 2015. This approach reduced the related operational risks in the overall migration process. User committees are organised on a regular basis where such things as the impact of the migration to T2S is discussed, including settlement fail rates [2].

(1) Source: ECB Blue Book, 2015 data.
(2) Minutes of NBB-SSS User Committees are available at https://www.nbb.be/en/payment-systems/securities-settlement-system-nbb-sss.

CHART 7 SECURITIES DEPOSITS AND SETTLEMENT TURNOVER IN NBB-SSS



Source: NBB.

Euroclear Belgium

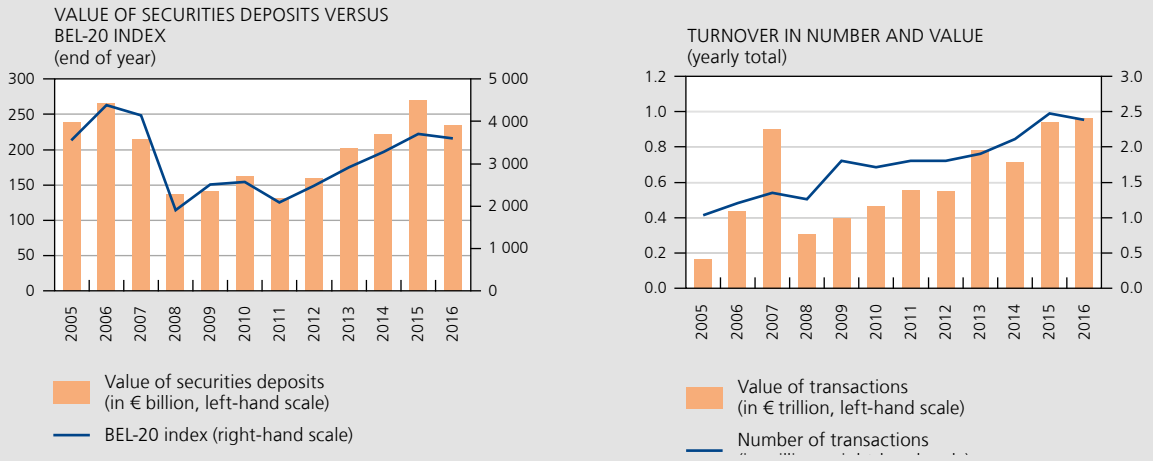
More than 99 % of securities deposits held in Euroclear Belgium are Belgian equities. As these are valued at market prices, the value of securities deposits fluctuates with market volatility. At the end of 2016, the total value of securities deposits held in Euroclear Belgium stood at € 235 billion (down 12.8 % from € 269 billion). Since about 80 % of these deposits are BEL-20 equities, the value of securities deposits follows in general trends in the BEL-20 index (chart 8,

left-hand panel). In terms of turnover, the number of transactions processed decreased by 3.6 % (from 2.48 to 2.39 million), whereas the value of transactions settled increased slightly with 2 % (from € 945 to € 964 billion) (chart 8, right-hand panel). On average, Euroclear Belgium processes daily about 9,350 transactions with a value of € 3.78 billion.

Euroclear Belgium's settlement activity is integrated in a joint platform with Euroclear France and Euroclear Nederland; i.e. the Euroclear Settlement of Euronext-zone Securities system (ESES). Besides a common IT platform, these ESES CSDs share harmonised settlement and custody services, and apply a harmonised Euroclear services pricing model. Daily settlement operations of Euroclear Belgium are outsourced to T2S since September 2016. As Euroclear Belgium's business is primarily in equities, unlike the other ESES CSDs in which also government securities are held, the share of Euroclear Belgium in ESES is rather limited (1).

(1) In terms of securities deposits in value, Euroclear Belgium accounted for 3.1 % of the aggregate value held by ESES CSDs at year-end 2016.

CHART 8 SECURITIES DEPOSITS AND SETTLEMENT TURNOVER IN EUROCLEAR BELGIUM



Source: Euroclear.

Box 2 – TARGET2-Securities

TARGET2-Securities (T2S) is a pan-European common platform of 20 EU CSDs for securities settlement in central bank money operated by the Eurosystem (1). As shown in the table below, European CSDs have been migrating their settlement activity to the T2S platform in several waves, starting in 2015. There were two migration waves in 2016. During Wave 2 in March, the NBB-SSS and Interbolsa (Portugal) migrated their settlement platform to T2S. Wave 3 in September included the ESES CSDs (i.e. Euroclear France, Euroclear Nederland and Euroclear Belgium) as well as VP Lux (Luxembourg) and VP Securities (Denmark). In February 2017, migration Wave 4, including a.o. the German and Austrian CSDs, was completed successfully. The final wave was scheduled for September 2017. Euroclear Finland announced in January 2017 that its migration to T2S will have to be rescheduled to a later date still to be confirmed.

(1) More information about T2S can be found on the ECB's website: https://www.ecb.europa.eu/paym/t2s/html/index.en.html.

T2S MIGRATION PLAN

Wave 1 22-06-2015 – 31-08-2015	Wave 2 29-03-2016	Wave 3 12-09-2016	Wave 4 06-02-2017	Wave 5 18-09-2017
Bank of Greece Securities Settlement System (BOGS)	Interbolsa (Portugal)	Euroclear Belgium	Centrálny depozitár cenných papierov SR CDCP (Slovakia)	Baltic CSDs (Estonia, Latvia, Lithuania)
Depozitarul Central (Romania)	National Bank of Belgium Securities Settlement System (NBB-SSS)	Euroclear France	Clearstream Banking Frankfurt (Germany)	Iberclear (Spain)
Malta Stock Exchange		Euroclear Nederland	KDD – Centralna klirinško depotna družba (Slovenia)	
Monte Titoli (Italy)		VP Lux (Luxembourg)	KELER (Hungary)	
SIX SIS (Switzerland)		VP Securities (Denmark)	LuxCSD (Luxembourg)	
			OeKB CSD (Austria)	

Source: ECB.

BUSINESS ACTIVITY

In December 2016, T2S settled about 5.3 million transactions on a monthly basis; a daily average of 254 724 transactions. In March 2017, after CSD migration Wave 4, the number of transactions settled on T2S more than doubled up to 11.5 million transactions or, on average, 498 655 transactions per day. Including Wave 4, T2S is currently processing 90 % of the expected volume for 2017.

OVERSIGHT APPROACH

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 T2S enables the member CSDs to comply with the regulations applicable to them. In line with PFMI Responsibility E (Cooperation with other authorities) of the CPMI-IOSCO Principles for Financial Market Infrastructures (PFMIs), 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.

SUPERVISORY PRIORITIES IN 2017

One of the priorities for the T2S overseers and supervisors is the next migration of CSDs joining T2S. The CSD Regulation (CSDR) imposing new requirements on EU CSDs will also take up a considerable amount of regulatory

attention in order to make sure that the current set-up of T2S does not hinder, or even more supports the CSDs in their effort to become CSDR compliant. In that regard, T2S could develop common tools (such as a tool to calculate the penalties for settlement fails), instead of each individual CSD making IT adjustments to be CSDR compliant.

Role of Belgian (I)CSDs in the mobilisation of collateral

Euroclear Group entities, including Euroclear Bank, provide collateral management services as a triparty agent, in which it takes over the collateral management tasks (including collateral selection, valuation and substitution) from its participants during the lifecycle of the transaction concluded between two participants. The Euroclear "Collateral Highway" aims to establish a common pool of collateral assets to serve the needs of their holders. Collateral supply fragmented across various holding locations can be aggregated by sourcing collateral from other (I)CSDs and custodian banks where the assets are held (i.e. highway "entries"). Once collateral is sourced into the Euroclear system, participants can allocate it to their counterparties to support a range of transactions, including central bank operations, repos, securities lending or margins for CCPs (i.e. highway "exits"). As shown in chart 9 (left-hand panel), at group level, the average daily value of triparty collateral managed by the Euroclear (I)CSDs by the end of 2016 had reached more than € 1 trillion, slightly 0.4 % up from 2015.

Euroclear Bank and NBB-SSS play an important role in the mobilisation of collateral for monetary policy purposes[1]. Via Euroclear Bank, eligible Eurobonds and domestic assets held on a cross-border basis via eligible links to other (I)CSDs can be mobilised within the Eurosystem. In the case of NBB-SSS, only Belgian eligible securities can be mobilised as it has no links with other (I)CSDs. As shown in table 6 below, based on daily average 2016 data, total collateral held in custody held by the Eurosystem central banks amounts to about € 1.7 trillion. Close to 30 % of this amount is collateral mobilised on a cross-border basis. Whereas the share of cross-border collateral mobilised by Belgian institutions is minor (1.8 %), the share that goes through Belgian (I)CSDs is about 24 % as illustrated in chart 9 (right-hand panel). This means that collateral assets held in NBB-SSS and Euroclear Bank (including Eurobonds) account for a large portion of cross-border collateral assets mobilised for monetary policy purposes by credit institutions in other euro area countries.

Collateral management is considered as a strategic business given regulatory initiatives triggering new collateral obligations for centrally cleared and non-centrally cleared OTC derivatives. In 2016, EMIR introduced mandatory central clearing of interest rate derivatives for a first set of counterparties (i.e. clearing members as from June 2016 and other counterparts with large derivatives volumes as from December 2016). EMIR's central clearing mandate will be further extended to other counterparties as from June 2017. For non-centrally-cleared OTC derivatives, BCBS-IOSCO's new initial margin (IM) requirements are being gradually applied, starting in countries such as the United States and Japan since 1 September 2016, while the variation margin (VM) requirements are applicable as from March 2017.

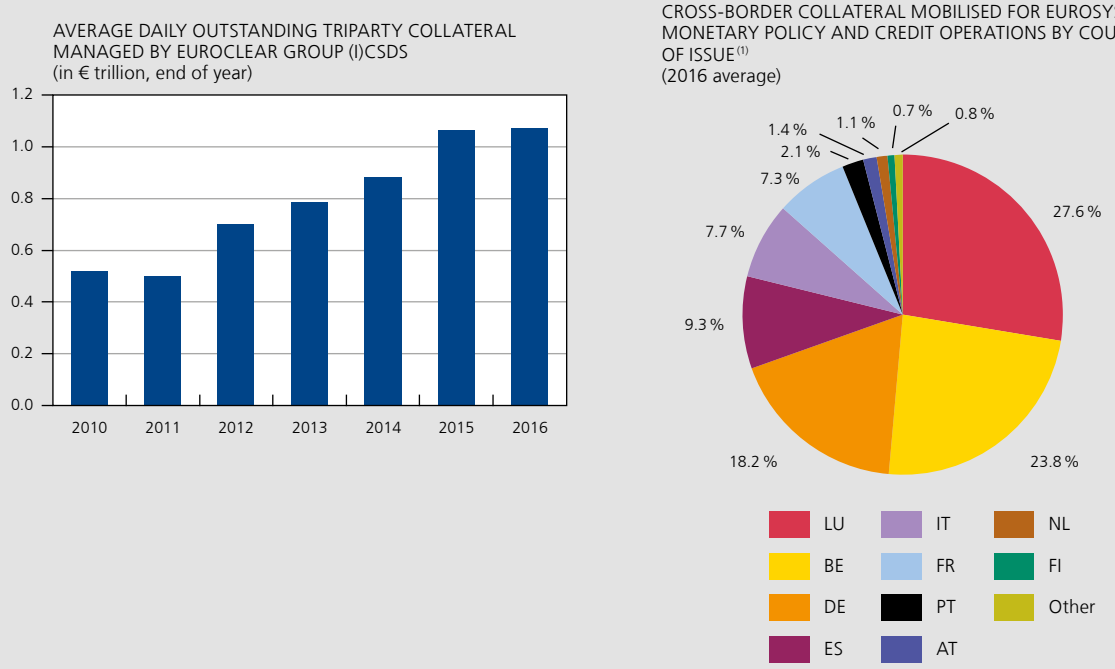
One cornerstone of Euroclear Group's collateral strategy is the joint venture with the Depository Trust & Clearing Corporation (DTCC), so-called DTCC-Euroclear GlobalCollateral Ltd. The new service offerings are being delivered in subsequent phases. As of March 2017, GlobalCollateral Ltd enables market participants to mobilise securities cross-border from the US to Europe for use as collateral. In practice, participants can use their Depository Trust Company (DTC) eligible USD assets – including US equities, corporate bonds and asset backed securities – for securities financing transactions within Euroclear Bank. In a next project delivery phase, scheduled for 2017, the scope of assets that can be mobilized through this gateway will be extended with US government bonds and participants will be able to automatically select and optimise their collateral portfolio across multiple counterparties and exposures.

Another deliverable is a solution to provide straight-through processing for the settlement of margin obligations for non-centrally cleared derivatives transactions. It is anticipated that usage of the new service will take-off in the first half of 2017 when rules for non-centrally cleared derivatives will be applicable. Up until now, margin calls have often been a manual process for some counterparties, opening up operational risks which would further increase when regulation

(1) Assets held in Euroclear Belgium are mainly equities and therefore not eligible as collateral for monetary policy purposes.

comes fully into effect. Automated settlement of margin obligations thus aims to improve operational and liquidity risk management. In July 2016, two institutions – State Street and Northern Trust – confirmed their participation in a pilot program to test the new service.

CHART 9 ROLE OF BELGIAN (I)CSDs IN THE MOBILISATION OF COLLATERAL



Sources: Euroclear, ECB.
(1) The country of issue specifies which countries supply the assets that are used cross-border.

TABLE 6 COLLATERAL HELD IN CUSTODY BY THE EUROSYSTEM

(average, based on holdings on the last Thursday of each month in 2016)

	Market values after haircuts in € billion	In %
Total collateral held in custody by the Eurosystem	1 664.7	
Total cross-border collateral held in custody by the Eurosystem	483.5	29.0
of which:		
Cross-border collateral mobilised at Belgian (I)CSDs	115.4	23.9
Cross-border collateral mobilised by Belgian financial institutions	8.7	1.8

Source: ECB.

PRUDENTIAL & OVERSIGHT APPROACH

The Bank closely monitored preparations for and the actual migration of NBB-SSS (March 2016) and Euroclear Belgium (September 2016) to T2S. In the latter case, the ESES CSDs' overseers and market regulators (see box 3 on cooperative

arrangements for Euroclear) interacted intensively with ESES. Post-migration, due attention is being paid to changes in settlement fail rates. For NBB-SSS, they are higher than before migration to T2S (5.3 % in 2015 versus 7.1 % in 2016). In the case of Euroclear Belgium, fail rates were on average 2.0 % in Q4 2016 compared to 1.7 % in Q4 2015. CSDs are interacting with T2S operators on how to further improve settlement efficiency. Lower settlement efficiency rates are partly due to CSD participants' behaviour not yet being fully adapted to the new environment. It should also be added that, for NBB-SSS, a securities lending and borrowing service supporting settlement efficiency was no longer available in the T2S environment.

Cyber resilience remained a focus of the Bank and other Euroclear Group authorities. Further work was conducted on enhancements to Euroclear's overall cyber security posture and its "holistic" approach towards cyber resilience, including Board involvement, crisis communication procedures and human resources' policies and procedures (including the vetting process). NBB-SSS is also conducting a self-assessment against the CPMI-IOSCO guidance on cyber resilience. In the framework of recent cyber heists targeting the high-value transaction chain, the Bank has reviewed cyber security in end points of payment and securities settlement systems established in Belgium, including Euroclear SA, Euroclear Bank and Euroclear Belgium (see Chapter 4 on SWIFT and article on cyber security in financial market infrastructures).

For Euroclear Bank, the Bank has reviewed the PFMI assessment with regard to Principle 4 on credit risk and Principle 7 on liquidity risk. Credit use by participants in the system, which is secured and, as a rule, intraday, is the source of Euroclear Bank's liquidity needs. As it settles in multiple currencies, the link between credit and liquidity risk should be considered per currency. So far, the risk management framework has mainly been based on the available liquidity sources in EUR, supplemented by several liquidity arrangements for USD, GBP and JPY. This framework, which was basically targeting liquidity needs in the four major currencies (representing >95 % of settlement turnover in value terms), is being extended at the Bank's request to all relevant currencies eligible for cash settlement on Euroclear Bank's books, and based on the more specific CSDR requirements. The liquidity stress-testing framework is being upgraded accordingly.

Apart from a specific focus on credit and liquidity risk management, the Bank also carried out an in-depth analysis of risk governance aspects in Euroclear Bank, including the risk management function outsourced by the latter to Euroclear SA. For that purpose, Euroclear Risk Management was requested to provide a self-assessment based on 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(1) process(2). 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(3) 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 in the framework of the CSDR. In support of the implementation of these frameworks, current available tools will be further enhanced to allow the aggregation of risk data which is considered key to making informed decisions at Euroclear Group level. The risk management principles and guidelines referred to above also stipulate that the scope of risks covered by institutions' policies should not be limited to credit, market, liquidity and operational risks. In that respect, initiatives to build on capabilities and resources within Euroclear Risk Management with regard to systemic risks have been taken recently. The so-called three lines of defence (i.e. operations department as 1st line managing risks on a day-to-day basis, risk management as 2nd line monitoring material risks and internal audit as 3rd line providing an independent review of both 1st and 2nd line) are within scope of the analysis conducted by the Bank. Specific attention is given to the capability of the 1st line to define potential risk events and their corresponding risk responses. Risk management as 2nd line ought to challenge these risk responses within the boundaries set by the Risk Appetite Framework. Further follow-up work on risk governance by the Bank is envisaged in 2017.

The Bank has reviewed the recovery plans of Euroclear Bank and Euroclear SA (as assimilated settlement institution) based on the specific guidelines it published in August 2016. The revised versions of the recovery plans that were made available end 2016 will be further assessed by the NBB in the framework of the CSDR authorisation process.

(1) Internal capital adequacy assessment process.
(2) Including relevant principles and guidelines on applicable methodologies, risk management, internal corporate governance, risk data aggregation and reporting, and risk appetite frameworks from BCBS, EBA, ECB and FSB.
(3) Supervisory review and evaluation process.

Preparations made by Euroclear in support of the CSDR licensing process have been one of the central topics of prudential and oversight activities in 2016, both on a bilateral basis as well as on a multilateral basis among Euroclear Group authorities.

Box 3 – Cooperation between the Bank and other authorities with regard to Euroclear

Owing to the international scope of Euroclear's activities, the Bank cooperates with other authorities, either on a multilateral or bilateral basis, as summarised in the table below.

OVERVIEW COOPERATION WITH REGARD TO EUROCLEAR

	Rationale for cooperation
National cooperation	
Financial Services and Market Authority (FSMA)	Market authority responsibilities regarding CSDs in Belgium
International cooperation	
Euroclear SA/NV	
Euroclear Group overseers and market supervisors (BE: National Bank of Belgium (NBB), FSMA; FI: Bank of Finland, Finanssivalvonta; FR: Banque de France (BdF), 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
Central Bank of Luxembourg/Commission de Surveillance du Secteur Financier	Bilateral cooperation on the link between Euroclear Bank and Clearstream Banking Luxembourg ("the Bridge")
Securities Exchange Commission	Bilateral cooperation focusing on US-related activities within Euroclear Bank
Euroclear Settlement of Euronext-zone Securities (ESES)	
ESES overseers and market supervisors (BE: NBB, FSMA; FR: BdF, AMF; NL: DNB, AFM)	Multilateral cooperation joint settlement platform of Euroclear France, Euroclear Nederland and Euroclear Belgium.

SUPERVISORY PRIORITIES IN 2017

One of the main priorities for 2017 is the CSDR authorisation filing of Euroclear Bank and Euroclear Belgium. While Euroclear Belgium has to obtain a CSD licence under the CSDR, Euroclear Bank needs to obtain an authorisation to provide both (I)CSD and banking-type ancillary services. The interoperable link between Euroclear Bank and Clearstream Banking Luxembourg needs to be authorised as well. As competent authority under CSDR, the Bank is responsible for deciding on the authorisation. (I)CSDs are obliged to apply for authorisation no later than six months after the effective application date of the regulatory technical standards published in March 2017. If the application is considered incomplete, the Bank shall set a time limit by which the (I)CSD has to provide additional information. In the case of Euroclear Belgium which shares a settlement platform with Euroclear France and Euroclear Nederland, respective national overseers and market regulators have agreed to coordinate the national authorisation process of their respective CSDs.

Governance, with the Euroclear Group (I)CSDs having outsourced critical services to the parent holding company (Euroclear SA), is a key aspect in the CSDR authorisation process. The PFMIs had already indicated its importance for FMIs that are part of a larger organisation having clear governance arrangements, notably with regard to conflicts of interest and outsourcing issues. In addition, an FMI which relies upon or outsources part of its operations to another FMI or service provider should have timely access to information, as well as proper controls and monitoring tools in place. Although these principles have also been adopted in the CSDR and related ESMA standards, the latter is more specific about the access of information to authorities and the need for the CSD to remain in control of the management of the risks it faces. In addition to the PFMIs, the competent and relevant authorities of the outsourcing CSDs can have access to the information directly from the outsourcee (in casu Euroclear SA) to allow them to assess the outsourced activities' compliance with CSDR.

In parallel with the preparation of the CSDR authorisation process, the Bank will further review and update the PFMI assessment of Euroclear Bank. It will take into account new available guidance to the PFMIs with regard to operational risk (including cyber resilience) and risk management (including recovery and resolution). Further attention will also be paid to the role of Euroclear Bank in collateral management services which are expected to grow due to the implementation of EMIR. Common interests at group level (i.e. governance, risk management, cyber resilience, outsourcing) will be further discussed among Euroclear overseers and securities regulators.

2.3 Custodians

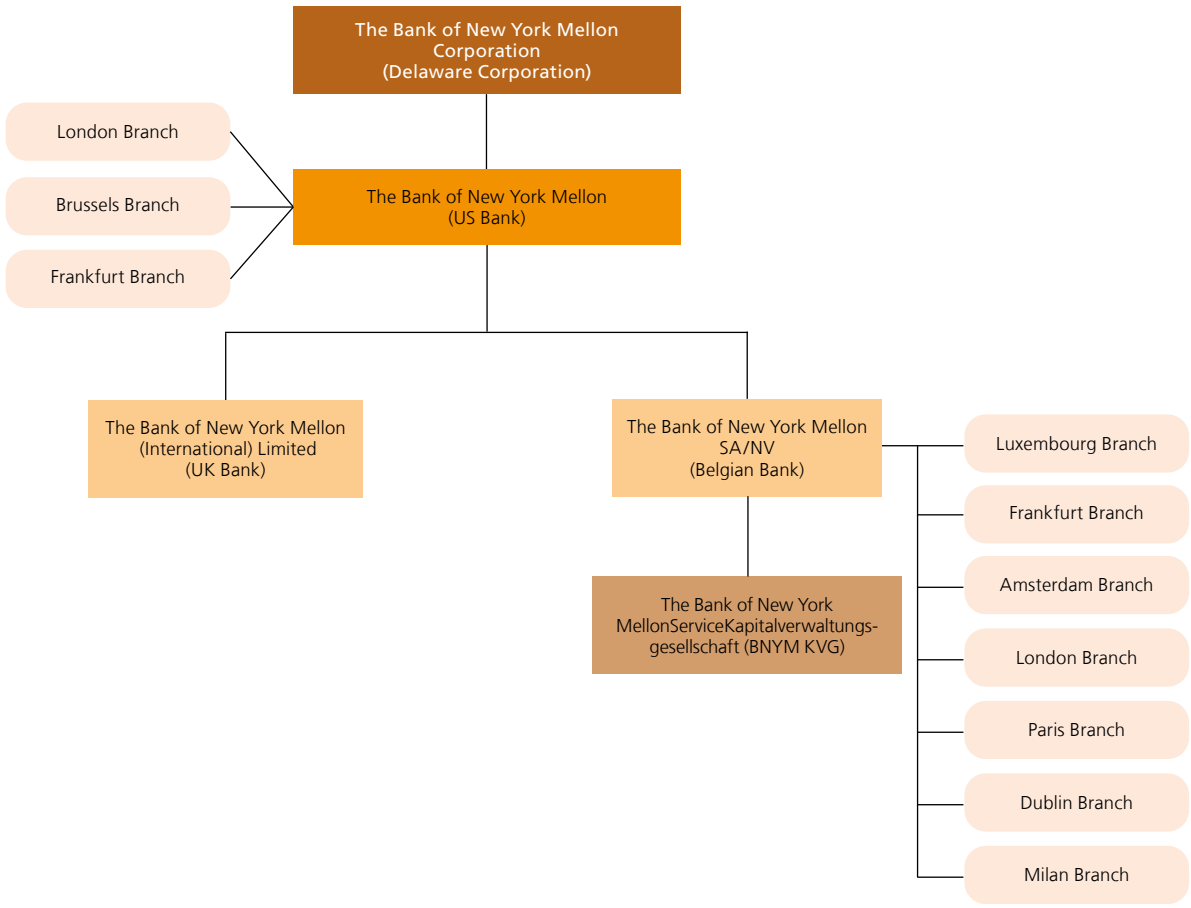
Custodians facilitate access to the securities investment market by providing securities investment related services (e.g. custody, asset administration, tax and foreign exchange services, collateral management, securities financing) to institutional investors or financial service providers in the investment chain. Custodian banks have a distinct risk profile from other financial institutions as their business lines all relate to the investment servicing activity for professional counterparties. They do not engage in retail banking, in significant maturity transformation activities, nor in proprietary trading. As such, they are considered as part of the payment, clearing and settlement ecosystem. This is explained in more detail in box 4.

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 Group). 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. As shown in chart 10, BNYM SA/NV has a non-bank subsidiary in Germany and branches in Luxembourg, Germany, the Netherlands, the UK, France and Ireland, 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), initiated before the US resolvability enhancement requirements were issued, and has recently been completed by integrating a Luxembourg subsidiary and Italian branch of the group in BNYM SA/NV.

The BNYM Group is also present in Belgium through a branch of the US parent company and through a CSD which is also a subsidiary of the parent company[1]. The Brussels branch has outsourced all its operational activities to BNYM SA/NV (the Brussels branch essentially hosts the cash and securities accounts of clients that cannot be deposited in a non-US bank).

(1) Not shown in chart 10. BNYM SA/NV has indicated that BNYM CSD will not file for a licence under the CSD Regulation.

CHART 10 BNYM GROUP STRUCTURE AND BNYM SA/NV POSITION
(simplified diagram)



Box 4 – Specific risk profile of a custodian

A custodian's core services are to hold and safekeep securities for investors, provide record keeping services, receive interest, dividend and redemption payments, withholding tax on behalf of its clients. Assets held under custody are recorded off balance sheet and therefore the failure of a custodian would not result in the loss of customers' securities.

Apart from these core services, custodians may offer complementary services in order to facilitate clients' investment in securities and portfolio management as, for example, foreign exchange services, collateral management as well as

securities lending. In those activities, the custodian acts upon its clients' instructions. Custodians may also allow short term cash overdrafts to ensure timely settlement of securities purchases in case of operational delays in client funding.

Credit institutions typically take short-term deposits and use them to fund long term loans. Net interest income is the bulk of a credit institution's income. Unlike credit institutions, custodians do not engage in significant maturity transformation activities. Their earnings are therefore not generated primarily from net interest income but rather from service fee revenues.

Custodians face market risk, operational risk, as well as credit and liquidity risk. The extent to which custodians face each of these risks varies significantly from typical credit institutions. Market risk is limited (as custodians' assets held under custody are recorded off balance sheet and belong to their clients). Operational risk, on the contrary, is high because of – among other factors – the dependence on sophisticated IT systems to process large volumes of transactions and operational tasks. In terms of credit risk, notwithstanding potential lower level and shorter-term risks, it can be observed that custodians are usually holding relatively higher levels of capital against their counterparties' exposures, in particular to cover for potential concentrations on systematically important counterparties. While they also face liquidity risk like other credit institutions, it has to be managed by custodians on an intraday basis maintaining sizeable portfolios of highly liquid assets.

In its capacity as supervisor, the Bank adopts a pragmatic and risk-based approach that fits the specific risk profile of these types of financial institutions.

CHANGES IN REGULATORY FRAMEWORK

As a bank, every change in banking regulation (Capital Requirements Directive, Capital Requirements Regulation, EBA guidelines, Bank Recovery and Resolution Directive, etc.) is applicable to BNYM SA/NV. Moreover, as its clients are exclusively institutional counterparties, BNYM SA/NV offers services and accompanying solutions to ensure compliance of its clients with the regulations that they themselves have to comply with (e.g. AIFMD[1], UCITS[2], Collateral Directive[3], etc.).

BUSINESS ACTIVITY

At group level, BNYM US is the largest custodian bank in the world with assets under custody worth about $ 30.5 trillion[4]. Acting as a global custodian for the group, BNYM SA/NV holds assets on behalf of other BNYM Group entities through worldwide relationships with 100+ sub-custodians or (I)CSDs. BNYM SA/NV facilitates the expansion of BNYM into other EU countries through the establishment of a network of branches or passporting of services (further detailed below).

By the end of 2016, BNYM SA/NV counted 1 840 clients which are all institutional counterparties ranging from traditional buy-side investors (insurance companies, pension funds, mutual funds, etc.) to investment banks, broker-dealers and hedge funds. Due to its role as the global custodian of the group, BNYM SA/NV clients' base, served

(1) EU regulation applicable to hedge funds, private equity funds and real estate funds for investor protection purposes. Directive 2011/61/EU of the European Parliament and of the Council of 8 June 2011 on Alternative Investment Fund Managers and amending Directives 2003/41/EC and 2009/65/EC and Regulations (EC) No 1060/2009 and (EU) No 1095/2010, OJ. 1 July 2011, L.174/1, 1-73. (http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011L0061&from=EN).

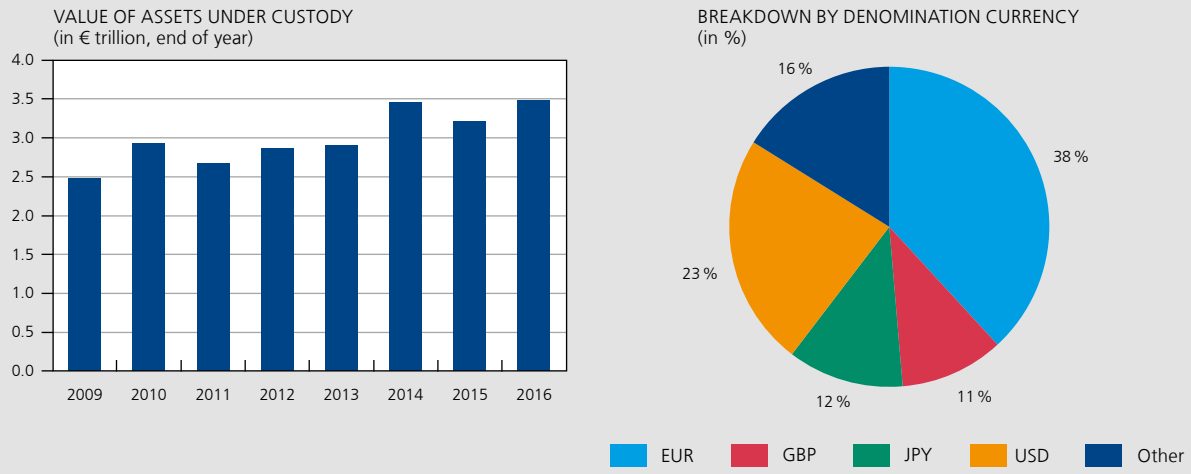
(2) EU regulation for the management and sale of mutual funds.Directive 2014/91/EU of the European Parliament and of the Council of 23 July 2014 amending Directive 2009/65/EC on the coordination of laws, regulations and administrative provisions relating to undertakings for collective investment in transferable securities (UCITS) as regards depositary functions, remuneration policies and sanctions, OJ. 28 April 2014, L.257/186, 1-28. (http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0091&from=EN).

(3) Directive 2002/47/EC of the European Parliament and of the Council of 6 June 2002 on financial collateral arrangements, OJ. 27 June 2002, L.168/43, 1-8 (http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0047&from=EN).

(4) At global level, the BNYM Group offers pre-trade, trade & post-trade services including investment management and investment servicing (including custody & asset servicing, funds administration). BNYM US has a key role of (duopolistic) US Treasury Bills Clearer with JP Morgan Chase (JPMC) to bring the US Treasury Securities to the market. About 85% of that activity flows through BNYM US and 15% through JPMC. The latter announced in July 2016 that it would withdraw from this business, which will result in a de facto monopoly of BNYM US. The operational implementation of JPMC's decision will take several months. BNYM is rated between AA- and AA+ by four credit-rating agencies.

directly or indirectly (i.e. through a group affiliate), is not only European but global. Chart 11 shows that BNYM SA/NV held close to € 3.5 trillion assets under custody on behalf of its international clients. An increase of 8.1 % compared to previous year (€ 3.2 trillion). The main part of these assets is denominated in EUR (38 %), followed by USD (23 %), JPY (12 %) and GBP (11 %).

CHART 11 VALUE OF ASSETS UNDER CUSTODY HELD BY BNYM SA/NV



Source: BNYM.

In general, the main drivers impacting the strategy of custodians concentrate along three main axes. Firstly, changes in regulation and increased regulatory focus result in de-risking complex banking and IT structures and deleveraging banking entities. Custodians also have to focus on client asset protection measures and the resilience and resolvability of legal entities, as well as on enhancing the operational continuity and sustainability of the supervised entities.

Secondly, custodians need to meet changing clients' behaviour and demands. Traditional clients of custodians have stepped up their focus on risk-adjusted returns and are increasingly interested in the Big Data of *inter alia* their transactions and collateral portfolio. They also require more advisory services to assist them to comply with new regulations. In order to extract, process and provide access to value added data for its clients, custodian banks are intensively exploring a vast array of FinTech solutions.

Thirdly, custodian banks need to modernise their IT landscape to cut costs (and thus increase returns) as demanded by shareholders and other investors. Business opportunities related to clients' requests for more data analysis on their transactions, be it due to new regulatory requirements or from an efficiency and profitability gains perspective, also require changes in custodians' legacy IT systems which are often designed for processing transactions and not for extracting related information. Moreover, like most other banking institutions in a low interest rate environment, custodians – even if their profits are generated more largely from fee income activities – have to maintain profitability, be it only for raising of bail-inable capital purposes as requested by the resolution regulations.

The precise nature of the impact of Brexit on carrying custody activities is not precisely clear yet, as it depends on the content of the arrangements to be concluded between the EU and UK and their impact not only on the custodians but also on the custodians' clients, which are for the moment still unknown. However, experience has shown that diverging regulations (e.g. Dodd-Frank versus EMIR) have had an impact on the location of activities of custodian groups.

PRUDENTIAL APPROACH

The BNYM Group has been designated as a global systemically important financial institution (G-SiFI) by the Financial Stability Board (FSB). BNYM SA/NV is the only material entity of the group within the euro area and is labelled as domestic systemically important financial institution (D-SIFI) following the BCBS criteria or, based on the related EBA guidelines, as Other Systemically Important Institution (O-SII)[1]. BNYM SA/NV is supervised by the ECB under the SSM as a significant credit institution". The Bank is still the sole supervisor of BNYM Brussels Branch.

There are currently three supervisory colleges for the BNYM Group: the European (EEA) College, the US (FSB) College and the Crisis Management Group (CMG), also set up according to the guidelines of the FSB. As a material entity within the group, BNYM SA/NV is included in the scope of the three colleges and therefore the Bank is a member of these three colleges, alongside the ECB and the UK Prudential Regulation Authority. The US regulatory authorities (the Federal Reserve Bank of New York and the Federal Deposit Insurance Corporation) chair the FSB and CMG Colleges.

Moreover, the Bank has direct supervision competence for BNYM SA/NV as a so-called "assimilated settlement institution"[2]. This specific Belgian status has been developed to ensure adequate supervision of entities that provide core services to (I)CSDs.

The main developments that have driven recent prudential supervisory activities can be grouped around three main axes. A first axis is the upgrading of BNYM SA/NV's organisation, management and risk and control framework in order to bring it into line with its supervisory status of a licensed credit institution when it was transformed from a branch to a subsidiary in 2009. Secondly, the establishment of BNYM SA/NV's appropriate autonomy level in a group context and direct oversight by the parent company. A third axis is the reduction in operational complexity and establishment of effective and robust oversight of intragroup outsourcing.

SUPERVISORY PRIORITIES IN 2017

Like other global custodians, the BNYM Group is engaged in the process of reducing its global footprint (i.e. decreasing the complexity of its group structure), partly to cope with regulatory pressures to reduce operational risks and enhance resolvability, but also to increase sustainability and profitability. In that regard, the BNYM Group was an early mover that has positioned itself very clearly from the outset in simplifying its structure, notably through the merger of its euro area's legacy entities into one single entity called BNYM SA/NV.

Another challenge closely followed up by the Bank includes the modernisation of legacy IT systems to allow for the development of new applications and functionalities as well as enhanced data gathering and processing for internal management information systems, risk management and business development purposes for custodians to comply with new regulatory requirements applicable to them or their clients.

Recovery and resolution planning (RRP) at global custodians presents some specificities due precisely to the global coverage of these groups as well as the intricacies of their operational platforms and applications. In this context, the following topics are of particular relevance: legal entity, operational processes and IT systems rationalisation, the setting up and location of so-called "intermediate holding companies" or "intermediate parent undertakings" (i.e. potential requirement to bring sub-entities of third country G-SiFIs established in the euro area under a common entity located in the euro area[3]), the relevance, consistency and effectiveness of measurement of the RRP indicators throughout the crisis continuum, the conditions for continued access to FMIs as well as the communication flows between the different global stakeholders.

(1) For BNYM SA/NV, the final O-SII buffer has been set at 0.75 % by the Bank.

(2) The status of "Assimilated Settlement Institution" has been introduced in Art. 23 § 7 of the Law of 2 August 2002 on the supervision of the financial sector and financial services and in the Royal Decree of 26 September 2005 on the legal status of settlement institutions and assimilated institutions,

(3) Proposal for a Directive of the European Parliament and of the Council amending Directive 2013/36/EU as regards exempted entities, financial holding companies, mixed financial holding companies, remuneration, supervisory measures and powers and capital conservation measures, 2016/0364 (COD) (https://ec.europa.eu/transparency/regdoc/rep/1/2016/EN/COM-2016-854-F1-EN-MAIN.PDF).z

3. Payments

The Bank has a broad responsibility in the area of payments and adopts two different regulatory roles over the payments landscape; i.e. oversight and prudential supervision as described in chart 12 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, prudential supervision pursues safe, stable and secure financial institutions delivering payment services to the users.

The interest of central banks for the payments landscape 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 a safe, reliable and competitive PSPs' environment in the country.

Section 3.1 describes the two payment systems which are core for the Belgian payment infrastructure: TARGET2 and the Centre for Exchange and Clearing (CEC). TARGET2 is the large-value payment system connecting Belgian banks with other European ones for processing high-value payments and serves as the basic connecting infrastructure needed for the implementation of central bank monetary policy. CEC is the domestic retail payment system processing intra-Belgian domestic payments. CLS Bank, a payment-versus-payment (PvP) settlement system for foreign exchange (FX) transactions, is included in this section as well.

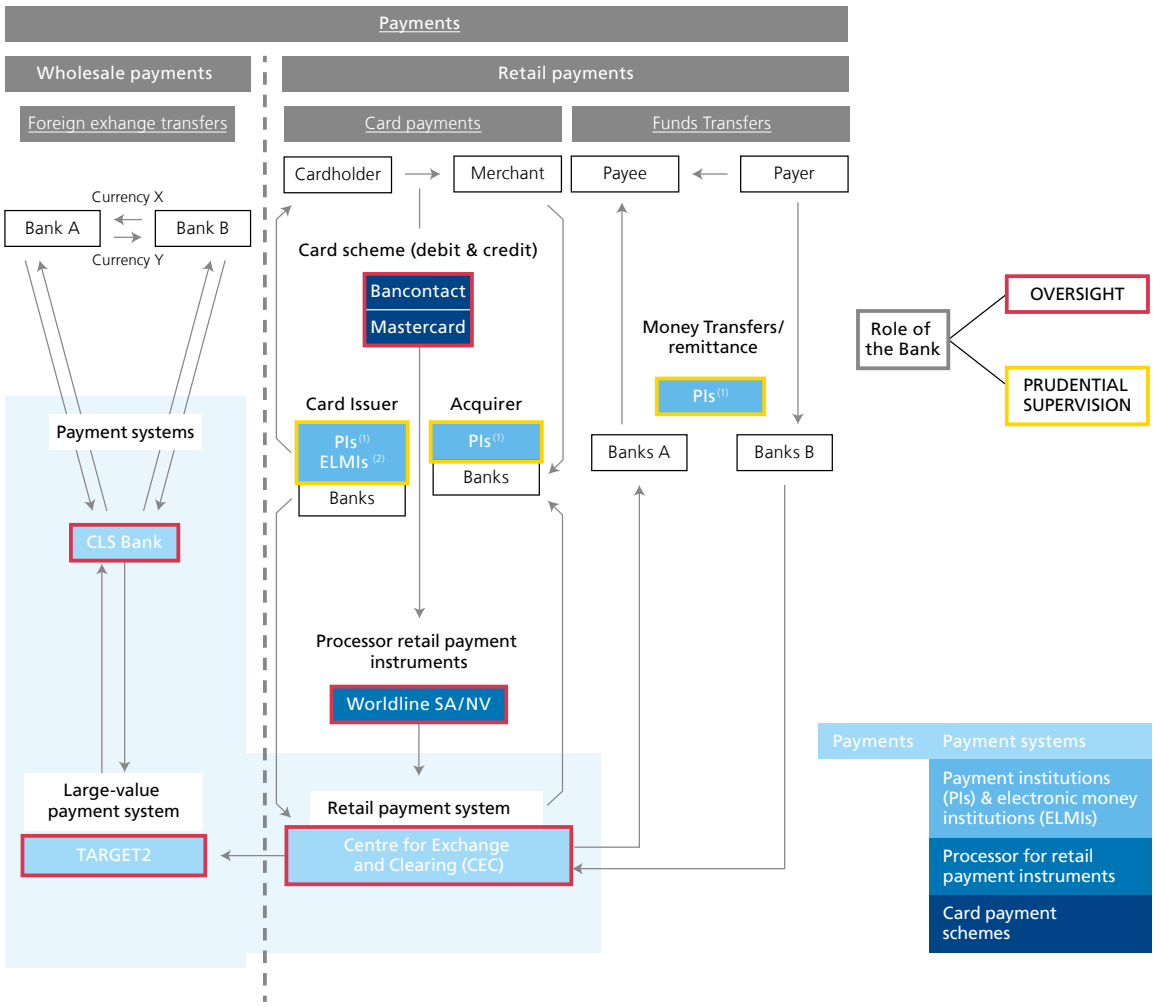
Prudential supervision of payment institutions (PIs) and electronic money institutions (ELMIs) – a relatively new sector for payment services which may offer since 2009, just like banks, payment services in Europe – is depicted in section 3.2.

As processor and acquirer[3] of retail payment instruments in Belgium, Worldline SA/NV is subject to both oversight and prudential supervision by the Bank. Section 3.3 explains this situation and the ongoing changes in the oversight regulatory framework in Belgium. This section looks at the synergies of the oversight and supervisory role a central bank can exert.

Section 3.4 covers the two payment card schemes overseen by the Bank: the domestic Bancontact scheme and the international Mastercard scheme. The Bank also contributes, indirectly, to other payment instrument oversight through the cooperation within the Eurosystem.

(1) A payment instrument is a tool to initiate payments of which currently the most widely used are credit transfers, cards and direct debits.
(2) A payment scheme is 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.

CHART 12 SCOPE OF THE BANK'S OVERSIGHT AND PRUDENTIAL SUPERVISION ROLE IN PAYMENTS LANDSCAPE



(1) Payment Institutions (PIs)
- *Card acquiring and processing: Alpha Card, Alpha Card Merchant Services, Bank Card Company, B+S Payment Europe, Instele, Rent A Terminal, Worldline SA/NV*
- *Money Transfers/Remittance: Africash, Belgian Money Corp, Belmoney Transfert, Gold Commodities Forex, HomeSend, Money International, MoneyTrans Payment Services, Munditransfers, Travelex*
- *Direct Debit: EPBF*
- *Hybrid: BMCE EuroServices, Cofidis, eDebex, FX4BIZ, Oonex, PAY-NXT, Santander CF Benelux*

(2) Electronic Money Institutions (ELMIs)
- *Buy Way Personal Finance, Fimaser, HPME, Imagor, Ingenico Financial Solutions, Ingenico Payment Services, Loyaltek Payment Systems, Orange Belgium, RES Credit*

3.1 Payment systems

This section covers both large-value payment systems (LVPS) and retail payment systems (RPS). Most payments made in Belgium are cleared and/or settled through TARGET2, the LVPS, and CEC, the Belgian domestic RPS. CLS Bank is included in box 6.

CHANGES IN REGULATORY FRAMEWORK

The regulatory framework applicable to systemically important payment systems (SIPS), covering both LVPS and RPS, is set out in the ECB Regulation on oversight requirements for SIPS[1], which in turn is based on the Principles for

(1) Regulation of the European Central Bank (EU) No 795/2014 of 3 July 2014 on oversight requirements for systemically important payment systems (ECB/2014/28), *OJ.* 23 July 2014, L.217/16, 1-15 (https://www.ecb.europa.eu/ecb/legal/pdf/oj_jol_2014_217_r_0006_en_txt.pdf)

Financial Markets Infrastructures (PFMI) published by CPMI-IOSCO in April 2012. It creates a strict level playing field for oversight on the SIPS in the euro area. SIPS are identified based on a set of quantitative and qualitative criteria as detailed in box 5.

Only SIPS are subject to the binding legal framework of this European regulation. For the other payment systems, the Eurosystem undertook a comprehensive review of the oversight standards for euro RPS (originally adopted in June 2003) and published in February 2016 the Revised Oversight Framework for RPS[1]. Besides the SIPS defined in the ECB Regulation (qualified as SIRPS in the context of RPS), this revised framework for RPS creates two additional categories of payment systems, i.e. the prominently important retail payment systems (PIRPS) and other retail payment systems (ORPS), identifying the sub-set of PFMIs applicable to each of them. As explained in box 5, to qualify as a PIRPS, the payment system's market share should at least be 25 % of total euro-denominated payments by volume at the level of a Member State whose currency is the euro. On the basis of this threshold, the CEC has qualified as a PIRPS. Although its market share even exceeds the threshold of 75 % that is required to qualify as a SIPS, the CEC does not meet any of the other mandatory criteria for SIPS and can consequently not be included in that category.

(1) ECB (2016), Revised oversight framework for retail payment systems (http://www.ecb.europa.eu/pub/pdf/other/revisedoversightframeworkretailpaymentsystems201602.en.pdf).

Box 5 – Payment systems oversight

In the Eurosystem, the oversight of systemically important payment systems (SIPS) is ruled by the ECB Regulation 795/2014 of 3 July 2014 on oversight requirements for SIPS[1]. It covers both large-value payment systems (LVPS) and retail payment systems (RPS) of systemic importance. According to this Regulation, a payment system is identified as SIPS if:

(a) it is eligible to be notified in the framework of the Settlement Finality Directive[2] and;
(b) at least two of the following occur over a calendar year:
- Total daily average value of euro-denominated payments processed is at least € 10 billion;
- Market share is at least 15 % of total volume of euro-denominated payments or 5 % of total volume of euro-denominated cross-border payments or 75 % of total volume of euro-denominated payments at the level of a Member State whose currency is the euro;
- Cross-border activity involves at least 5 countries and generates a minimum of 33 % of the total volume of euro-denominated payments processed by that SIPS;
- The system is used for the settlement of other FMIs.

The four SIPS identified in the euro area are TARGET2 operated by the Eurosystem, the pan-European LVPS and RPS set up by the private sector and operated by EBA Clearing (resp. EURO1 and STEP2), as well as the French RPS system CORE(FR). The Regulation states that the SIPS must comply with all the 2012 CPMI-IOSCO Principles for Financial Markets Infrastructures (PFMIs) applicable to payment systems (17 PFMIs out of 24 as shown in the Table below; other PFMIs are applicable to other types of FMIs, such as securities settlement systems, CSDs, CCPs or trade repositories).

In addition to the Regulation, the Eurosystem reviewed the oversight standards for euro RPS dating from June 2003 and published the Revised Oversight Framework for RPS in February 2016[3]. As well as the SIPS (qualified as SIRPS in the context of RPS), the framework further categorises RPS by introducing the prominently important retail payment systems (PIRPS) and other retail payment systems (ORPS). A non-systemically important RPS is a PIRPS if

(1) Regulation of the European Central Bank (EU) No 795/2014 of 3 July 2014 on oversight requirements for systemically important payment systems (ECB/2014/28), OJ. 23 July 2014, L.217/16, 1-15. (https://www.ecb.europa.eu/ecb/legal/pdf/oj_jol_2014_217_r_0006_en_txt.pdf).
(2) Directive 98/26/EC of the European Parliament and of the Council of 19 May 1998 on settlement finality in payment and securities settlement systems, *OJ*. 11 June 1998, L. 166, 45-50 (http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31998L0026&from=EN).
(3) ECB (2016), *Revised oversight framework for retail payment systems* (http://www.ecb.europa.eu/pub/pdf/other/revisedoversightframeworkretailpaymentsystems201602.en.pdf).

its market share is 25 % or higher of total euro-denominated payments by volume at the level of a Member State whose currency is the euro. Below that threshold, it will be considered as an ORPS.

The table below identifies the set of PFMIs applicable to each category of payment system. Whereas SIPS and SIRPS need to comply with all PFMIs relevant for payment systems, a subset thereof is applicable to PIRPS and ORPS.

OVERSIGHT FRAMEWORK FOR PAYMENT SYSTEMS: APPLICABLE CPMI – IOSCO PRINCIPLE BY CATEGORY

CPMI-IOSCO Principles for financial market infrastructures (PFMIs)	SIPS/SIRPS [1]	PIRPS [2]	ORPS [3]
Principle 1: Legal basis	X	X	X
Principle 2: Governance	X	X	X
Principle 3: Framework for the comprehensive management of risks	X	X	X
Principle 4: Credit risk	X		
Principle 5: Collateral	X		
Principle 6: Margin	n.	n.	n.
Principle 7: Liquidity risk	X		
Principle 8: Settlement finality	X	X	X
Principle 9: Money settlements	X	X	
Principle 10: Physical deliveries	n.	n.	n.
Principle 11: Central securities depositories	n.	n.	n.
Principle 12: Exchange-of-value settlement system	n. [4]	n.	n.
Principle 13: Participant-default rules and procedures	X	X	X
Principle 14: Segregation and portability	n.	n.	n.
Principle 15: General business risk	X		
Principle 16: Custody and investment risks	X		
Principle 17: Operational risk	X	X	X
Principle 18: Access and participation requirements	X	X	X
Principle 19: Tiered participation arrangements	X		
Principle 20: FMI links	n.	n.	n.
Principle 21: Efficiency and effectiveness	X	X	X
Principle 22: Communication procedures and standards	X	X	
Principle 23: Disclosure of rules, key procedures, and market data	X	X	X
Principle 24: Disclosure of market data by trade repositories	n.	n.	n.

Sources: ECB, NBB.
(1) SIPS/SIRPS: Systemically Important Payment Systems/Systemically Important Retail Payment Systems.
(2) PIRPS: Prominently Important Retail Payment Systems.
(3) ORPS: Other Retail Payment Systems.
(4) Art. 11 of the Regulation of the European Central Bank (EU) No 795/2014 of 3 July 2014 refers to payment versus payment. Current SIPS/SIRPS operators do not use a payment versus payment mechanism.

BUSINESS ACTIVITY

TARGET2

TARGET2, the large-value central bank payment system, is the largest payment system in the euro area in value terms, processing more than 90 % of the total value settled by LVPS in euro. As a SIPS, it serves as the backbone for other FMIs as it settles in central bank money the cash positions in euros of 74 so-called ancillary systems i.e. systems in

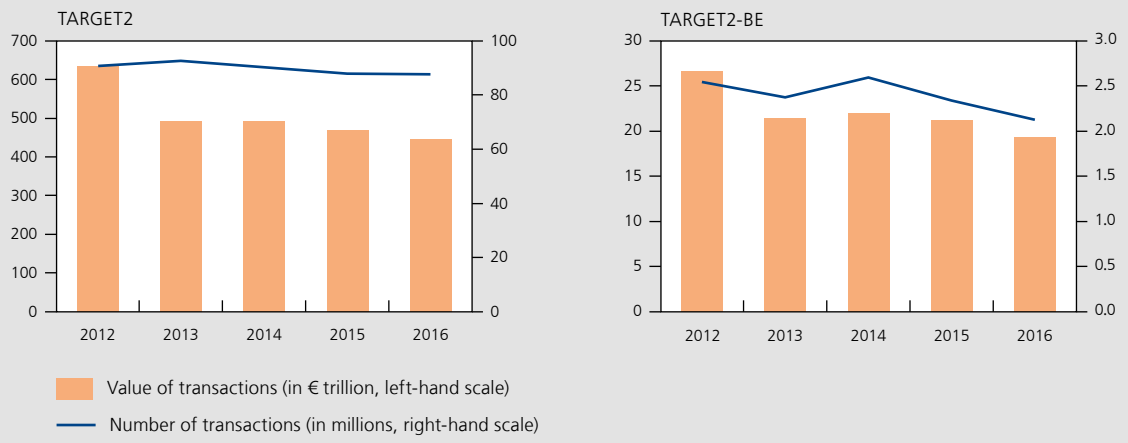
which payments or securities are exchanged and/or cleared whereas the ensuing monetary obligations are settled in TARGET2 (e.g. domestic RPS as the CEC, pan-European systems operated by EBA Clearing which is the private sector-owned provider of the RPS STEP2 and the LVPS EURO1, as well as (I)CSDs and CCPs).

As illustrated in chart 13 (left-hand side), the total value of transactions processed by TARGET2 in 2016 amounted to almost € 445 trillion (€ 1.735 trillion per day on average). The observed decline of 5 % on 2015 can be attributed to a lower volume of ancillary system transactions resulting from the migration of additional CSDs to the TARGET2-Securities platform. The total volume of payments processed was close to 88 million transactions (about 341 000 payments per day on average) and remained unchanged compared to the previous year.

At the end of 2016, 21 participants out of 1 067 direct participants of TARGET2 were Belgian financial institutions. Chart 13 (right-hand side) shows that about 2.13 million transactions related to TARGET2-BE, the Belgian component of TARGET2 [1], representing a value of € 19.3 trillion. TARGET2-BE represents 4.34 % of the total value processed by the TARGET2 system and 2.43 % of the total volume.

CHART 13 NUMBER AND VALUE OF TRANSACTIONS PROCESSED BY CEC AND TOP-10 EURO AREA DOMESTIC RETAIL PAYMENT SYSTEMS BY VALUE

(yearly total)



Sources: ECB and NBB.

Centre for Exchange and Clearing (CEC)

Although the CEC is not a systemically important infrastructure, it plays a crucial role in the Belgian economy as the central point for the clearing and settlement of retail payments, which mostly involve card payments, credit transfers and direct debit payments.

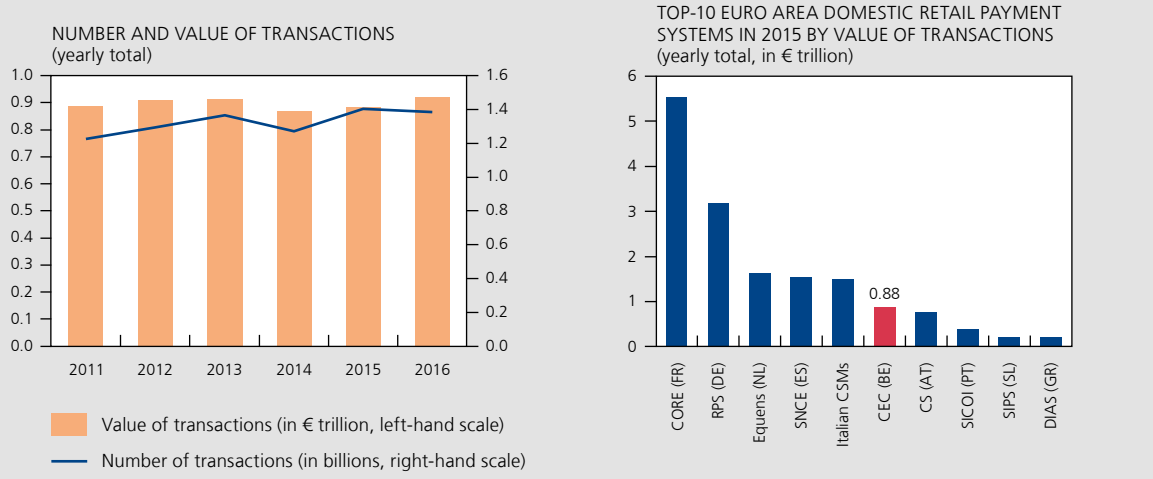
As shown in chart 14 below (left-hand panel), the CEC processed about 1.38 billion transactions in 2016 which is 1 % less than in 2015. The total value of the transactions processed by the CEC in 2016 amounted to € 0.92 trillion which is an increase of about 4 % compared to the € 0.88 trillion handled in 2015. Based on 2015 data, the CEC is the sixth largest domestic euro-denominated RPS in terms of value of transactions processed (chart 14, right-hand panel).

The main development concerning the CEC in 2016 is the ongoing instant payments [2] project. Regarding the operation of the future system, a Letter of Intent has been signed with STET, the French company to which the CEC

(1) TARGET2 is legally structured as a multiplicity of RTGS systems (TARGET2 component systems) where national central banks maintain their business relationships with domestic credit institutions.
(2) "Instant (or faster) payments" is the initiative towards payment systems settling retail payments in a real-time (or near real-time) on a 24-hour and 7-day basis as possible.

has outsourced its operations since 2013. The detailed features of this new payment mechanism will be clarified in the course of 2017.

CHART 14 NUMBER AND VALUE OF TRANSACTIONS PROCESSED BY CEC AND TOP-10 EURO AREA DOMESTIC RETAIL PAYMENT SYSTEMS BY VALUE



Sources: CEC and ECB.

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 (1).

In 2016, in addition to the regular oversight, a comprehensive assessment of TARGET2 has been conducted on the basis of the ECB Regulation on oversight requirements for SIPS (2). A disclosure report with the main findings of this assessment has been published in June 2016 on the ECB's website (3).

The Bank is responsible for the oversight of the CEC. In 2016, it started the assessment of the system against the 2016 Revised Oversight Framework for RPS as part of a Eurosystem-wide exercise. This assessment will be finalised in the course of 2017 after a peer review by the Eurosystem.

The French contractor STET relies on its infrastructure called CORE which is also used by the French RPS CORE(FR) overseen by Banque de France. In the context of this outsourcing, a cooperation framework has been agreed with Banque de France. The cooperation agreement is formalised in a Memorandum of Understanding (MoU) describing the exchange of information and oversight arrangements regarding aspects of common interest. The objective is to avoid any duplication of tasks for both overseers and market infrastructures.

OVERSIGHT PRIORITIES IN 2017

The work plan for the oversight of TARGET2 and other SIPS are defined at the level of the ESCB. In addition to the standard monitoring of the system (including new developments and risks), the 2017 continuous oversight annual cycle of TARGET2 will focus on the follow-up of the assessment. The Eurosystem is currently examining how the 2016

(1) The 20 euro area central banks (including the ECB) and five central banks from non-euro area countries: Bulgaria, Croatia, Denmark, Poland and Romania.
(2) During 2016, the Eurosystem conducted an oversight assessment of the four SIPS: TARGET2, EURO1, STEP2 and CORE(FR).
(3) ECB (2016), *Disclosure report – TARGET2 assessment against the principles for financial market infrastructures* (http://www.ecb.europa.eu/pub/pdf/other/t2disclosurereport201606.en.pdf).

CPMI-IOSCO Guidance on cyber resilience for FMIs, which clarifies how cyber risk should be assessed in the context of the PFMI, will be integrated into its oversight of payment systems.

In 2017, specific focus will be put on the CEC's cyber resilience. In particular, as for the other FMIs under its oversight responsibility, the Bank should assess inter alia the CEC's compliance with the customer security controls issued by SWIFT for better securing customers' connectivity to the SWIFT network. The Bank also intends to follow up on the development of the instant payments project more specifically from a risk perspective.

Implementation of the action plan resulting from the CEC assessment started in 2016 will also be covered.

Box 6 – CLS Bank

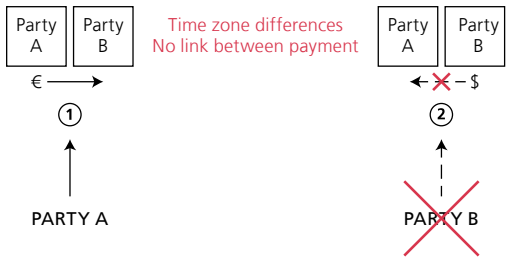
CLS Bank (CLS) is a US-based payment-versus-payment (PvP) settlement system for foreign exchange (FX) transactions in 18 currencies[1]. Without CLS (see chart below, left-hand side of top panel), FX transactions induce the risk that – due to time zone differences – one party wires the currency it sold but does not receive the currency

FUNCTIONING OF CLS

Elimination of FX settlement risk

FX Settlement without CLS

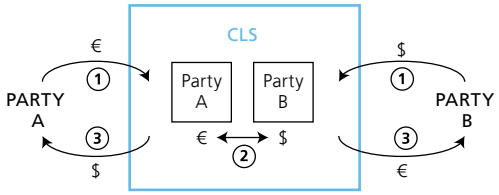
Party A sells € against $ to Party B



1. Party A wires € to Party B, before receiving $ later on.
2. When Party B defaults before wiring $, Party A suffers total loss (= principal risk → FX Settlement risk or "Herstatt risk") (after default Bankhaus Herstatt in 1974).

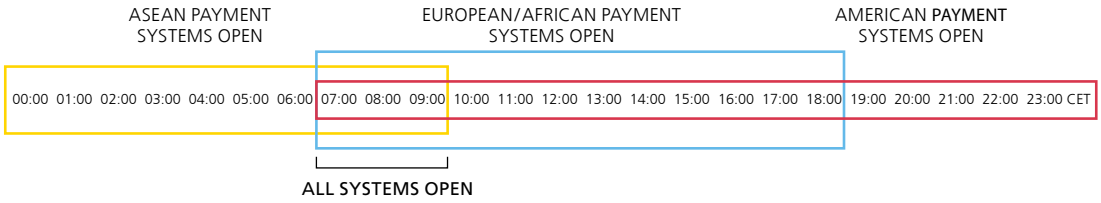
FX Settlement with CLS

Party A sells € against $ to Party B



1. Party A and B wire € resp. $ to CLS.
2. If both Party A and B have funded their CLS accounts, CLS will settle the transaction (simultaneous exchange = payment versus payment).
3. A and B receive their $ resp. € from CLS.

Common Settlement Window for CLS



(1) Australian dollar, Canadian dollar, Danish krone, euro, Hong Kong dollar, Hungarian forint, Israeli shekel, Japanese yen, Korean won, Mexican peso, New Zealand dollar, Norwegian krone, Singapore dollar, South African rand, Swedish krona, Swiss franc, UK pound and US dollar.

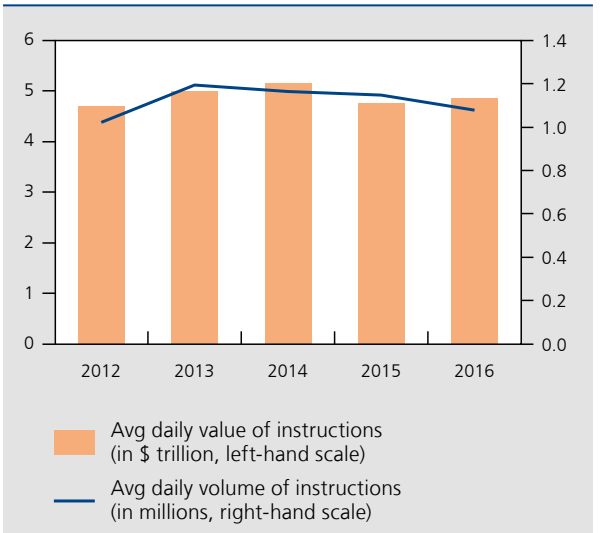
it bought from its counterparty. By settling transactions through linking the payments (PvP), CLS eliminates this FX settlement risk: i.e. if one party defaults and does not wire its currency to CLS, settlement will not take place and its counterparty will not lose its own currency (see chart above, right-hand side of top panel).

CLS has cash accounts at all central banks of the 18 CLS currencies (and thereby eliminates credit risk on commercial banks). The payment systems of these 18 currencies have a 2 hour overlap in their operating hours, i.e. a common settlement window from 07:00 AM to 09:00 AM CET (see chart above, bottom panel) during which CLS members can transfer to the CLS account the currencies they have sold (pay-ins by CLS member) and receive the currencies they have bought (pay-outs to CLS member). Pay-ins and pay-outs occur on a multilaterally netted basis, meaning that if Party A sold € for $ to Party B and bought € against £ from Party C, Party A only needs to pay/receive the net amount of its sales and purchases in €. Such netting reduces liquidity risk (as Party A does not need to transfer the gross amount of € to Party B) and operational risk (as netting reduces the number of transfers that need to be made).

BUSINESS ACTIVITY

CLS has more than 60 direct members among which many large international banks. There is currently one Belgian member in CLS (KBC). As shown in the chart below, average daily volume and value of instructions submitted to CLS have been rather stable. The average daily volume is slightly above 1 million, whereas the average daily value of instructions is close to $ 5 trillion equivalent.

AVERAGE DAILY VOLUME AND VALUE OF INSTRUCTIONS SUBMITTED TO CLS



Source: CLS.

According to calculations by CLS, 50.8% of global turnover in spot, outright forwards and FX swaps is settled through CLS. Reasons why FX transactions are not settled through CLS could be threefold:

– One or both of the currencies in the deal is not eligible for CLS. CLS is gradually expanding the list of currencies that can be settled in CLS. The Hungarian forint was the most recent addition (2015).

– One or both counterparties are not a member of CLS. While retaining strict risk-based criteria for accepting members, CLS has developed a non-shareholder membership which may make it easier for some banks to become a CLS member as the upfront investment in CLS shares is no longer required.
– As settlement in CLS happens when the opening hours of the payment systems of the 18 CLS currencies are overlapping, certain same-day FX transactions need to be settled outside CLS. CLS has already developed a Same-Day Session for US and Canadian dollar transactions.

OVERSIGHT AND PRUDENTIAL APPROACH

In 2012, CLS was 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. CLS is subject to the Federal Reserve Board's regulation, based on the CPMI-IOSCO Principles for Financial Market Infrastructures (PFMIs), establishing risk-management standards governing the operations related to the payment, clearing, and settlement activities of designated financial market utilities[(1)]. 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 5 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. The OC assesses the CLS system and any changes to it based on the relevant PFMIs.

OVERSIGHT PRIORITIES IN 2017

Besides the ongoing oversight by the OC, specific attention will be given to the follow-up of new CLS services. One of the new services that will be launched as of 2017 will be the CCP Settlement Service, a special platform for CCPs that clear FX transactions.

In addition, CLS is also taking measures with the aim of facilitating recovery and resolution of a member when needed. The "affiliate membership", for example, will allow entities that are part of the same corporate group as an existing CLS member to become members as well. This could make recovery and resolution of a complex group easier (as individual entities have direct access to CLS and are not dependent on another entity of the group) and allows members to comply with ring-fencing requirements where applicable.

(1) See https://www.federalreserve.gov/paymentsystems/reghh-about.htm.

3.2 Payment institutions and electronic money institutions

This section focuses on the prudential supervision conducted by the Bank on non-bank payment service providers (PSPs) for retail payments. Both payment institutions (PIs) and electronic money institutions (ELMIs) are non-banks providing respectively payment services and the issuing, redeeming and distributing of electronic money[(1)] in competition with banks. ELMIs may also provide payment services and given their ability to issue electronic money to the public are subject to a stricter prudential regime, e.g. stronger capital requirements[(2)].

(1) Electronic money (e-money) is electronically stored monetary value as a claim on the issuer which is issued on receipt of funds from the holder and which is accepted by a natural or legal person other than the electronic money issuer.
(2) As a rule, PIs have to maintain a capital of at least EUR 125,000. This is reduced to EUR 20,000 when the only payment service offered is money remittance and to EUR 50,000 when only the payment service provided by telecommunications service providers is offered or this latter is combined with money remittance. On top of that, PIs must calculate their "own funds" requirement as defined in the regulation and at all times maintain "own funds" sufficient to meet this requirement. ELMIs have to maintain, as a rule, a capital of at least EUR 350,000 and maintain 'own funds' equal (or higher) to 2 % of the outstanding issued e-money.

The regulatory and legislative framework for payment services was put in place in 2009 with the transposition of the European Payment Services Directive (PSD)[1] into the Belgian Law of 21 December 2009 on the legal status of PIs and ELMIs[2]. The goal of the Directive was to increase the level of competition in the payments market and to create a harmonised regulatory framework for payment services.

In order to ensure a common European framework, the Directive lists seven different types of payment services, ranging from the issuance of payment instruments to the remittance of money allowing retail customers to transfer cash to a third party abroad and vice versa[3].

There are three key developments in the payment services sector triggered by the PSD. A first one, is the introduction of the term *Payment Institution* (PI), which refers to firms who are granted a licence by a regulator within the European Economic Area (EEA) to provide one or multiple payment services[4]. A second important element of the PSD relates to the harmonisation of the prudential supervision regime across the EEA[5]. The framework for this regime is built upon authorisation requirements, covering among other things capital requirements and a specific governance structure with which applicants need to comply for obtaining a licence. Subsequently, the ongoing prudential supervision continues to verify whether these conditions are still being met. In order to be licensed, PIs and ELMIs need to demonstrate that they meet the authorisation requirements, listed in table 7 below.

TABLE 7 OVERVIEW OF AUTHORISATION REQUIREMENTS

- Identification details
- Programme of operations
- Business plan
- Evidence of initial capital
- Measures to safeguard the funds of payment service users
- Governance arrangements and internal control mechanisms
- Internal control mechanisms to comply with obligations in relation to money-laundering and terrorist financing
- Identity and suitability assessment of persons with qualified holdings in the applicant
- Structural organisation
- Identity and suitability assessment of directors and persons responsible for the management of the payment institution
- Identity of statutory auditors and audit firms

Source: NBB.

A third key influential addition from the PSD includes the "EU passporting process", which means that any PI licensed within the EEA is allowed to provide its services across the EEA.

(1) Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC, OJ. 5 December 2007, L. 319, 1-36 (http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32007L0064&from=en).

(2) Law of 21 December 2009 on the legal status of payment institutions and institutions for electronic money, on the access to the activity of payment service provider and the activity of issuing of electronic money and on the access to payment systems, Belgian Official Gazette 19 January 2010, 2.199.

(3) The PSD defines the seven types of payment services as follows:
(1) Services enabling cash to be placed on a payment account as well as all the operations required for operating a payment account.
(2) Services enabling cash withdrawals from a payment account as well as all the operations required for operating a payment account.
(3) Execution of payment transactions, including transfers of funds on a payment account with the user's payment service provider or with another payment service provider.
(4) Execution of payment transactions where the funds are covered by a credit line for a payment service user.
(5) Issuing and/or acquiring of payment instruments.
(6) Money remittance.
(7) Execution of payment transactions where the consent of the payer to execute a payment transaction is given by means of any telecommunication, digital or IT device and the payment is made to the telecommunication, IT system or network operator, acting only as an intermediary between the payment service user and the supplier of the goods and services.

(4) The PSD defines six different types of Payment Service Providers (PSPs): credit institutions, Payment Institutions (PIs), Electronic Money Institutions (ELMIs), European and national central banks, Member States or regional authorities and post office giro institutions.

(5) PSD does not only apply within the EU but it is also part of the EEA Agreement and therefore incorporated in national legislation of those countries.

Besides harmonising the payment services sector, the European Commission also adopted a standard set of rules for the issuance and management of electronic money. After having introduced a first Directive in 2000[1], which coined the term *Electronic Money Institution* (ELMI), a second piece of legislation was introduced in 2009[2]. This second Electronic Money Directive (EMD2) addresses issues such as the need of high capital requirements, the outdated definition of electronic money and the potential danger of an uneven level playing field across the EEA. EMD2 was transposed via a Belgian Law of 27 November 2012[3] and its stipulations integrated into the existing Law of 21 December 2009 on PIs to guarantee a common approach regarding the authorisation, operating conditions and performance of both PIs and ELMIs. Important to note is that ELMIs are authorised to provide all services in the scope of PIs. On the contrary, PIs are not allowed to issue electronic money.

CHANGES IN REGULATORY FRAMEWORK

Although the PSD and EMD2 took an important step in the consolidation of the regulatory framework of the European payments services sector, some regulatory inconsistencies and differences in interpretations that prevent the evolution towards a genuine level playing field are still in place. More specific, the 2012 Green Paper published by the European Commission[4] found that some new innovations in payment services operated in a legal vacuum and therefore lacked a minimal level of standardisation and interoperability.

In order to tackle these issues, a revised edition of the Payment Services Directive (PSD2) was adopted[5]. The amended Directive incorporates activities which are non-regulated so far but which will be considered as payment services from 13 January 2018 onwards (end of transposition period), i.e. *payment initiation services and account information services*. The new payment initiation services will require a licence as a PI while account information service providers need to be registered by the Bank. Both types of institutions will benefit from a lighter prudential regime as they are not coming into possession of clients' funds at any time in the payments process.

Besides introducing new payment services, the Directive also aims to ensure a high level of payment security by setting strict rules on when to use strong customer authentication. Moreover, PSPs will be subject to a notification duty in case of significant operational or security incidents. A European register, managed by the EBA, will be introduced to provide an overview of all the licensed PSPs in the whole EEA. Furthermore, cooperation requirements between the host and home country are enhanced and multiple definitions of the PSD are rewritten to be technologically neutral.

In order to safeguard the European-wide harmonisation and implementation of this Directive, the European Commission mandated the European Banking Authority (EBA) to launch the Task Force on Payment Services. This task force, in which the Bank participates, will deliver the necessary regulatory technical standards and guidelines with the aim to give detailed information to the market on how the PSD2 is to be understood and implemented in order to ensure a common European approach[6].

BUSINESS ACTIVITY

The Belgian payment services sector consists of a diverse set of actors, both foreign and local, that offer a wide range of technological solutions. In general, payment institutions with a full licence can be divided into the following four different types of businesses: i) card acquirers and processors, ii) money remitters, iii) direct debit institutions and iv) hybrid institutions.

(1) Directive 2000/46/EC of the European Parliament and of the Council of 18 September 2000 on the taking up, pursuit of and prudential supervision of the business of electronic money institutions, OJ. 27 October 2010, L. 275, 39-43 (http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0046&from=EN).

(2) Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions 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).

(3) Law to change the law of 21 December 2009 on the legal status of payment institutions, on the access to the activity of payment service provider and on the access to payment systems, and of other legislation on the legal status of payment institutions and of institutions for electronic money and of credit unions who are part of Crédit Professionel's network, Belgian Official Gazette 30 November 2012, 76.567.

(4) European Commission (2012), "Green Paper Towards an integrated European market for card, internet and mobile payments", COM/2011/0941, 1-25 (http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri= CELEX:52011DC0941&from=EN).

(5) 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 (http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=en).

(6) Regulatory technical standards cover the Directive as voted 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 however have to comply with these or publish the reasons for non-compliance.

Firstly, card acquirers and processors offer classic payment services such as the processing of card payments, the acquiring of merchants[1] or the renting of payment terminals. The second sub-set, money remitters, allows customers to transfer cash (remittance) from Belgium to a third party in different locations around the world and vice versa. In order to immediately supply the recipient with money, these institutions often have arrangements in place to have liquidity available in different locations. Thirdly, direct debit institutions manage the SEPA[2] direct debits of customers who have a mandate with a certain supplier to wire a person on a regular basis such as payments for utility bills. Lastly, hybrid institutions denote firms whose core activity does not fall under a classic payment service category or whose business model is not centered on offering payment services. A typical example is a consumer credit firm that issues pre-paid cards.

The Bank currently has 21 Belgian and 3 foreign PIs with a Belgian branch under its supervision. In order to stimulate innovation, the PSD also established a "waiver" regime that sets less stringent requirements on the minimum capital levels, as well as on the reporting procedure and the internal control mechanisms. The waiver cannot be used to passport the institution's services to other EEA members and it is only granted to PIs who remain below an average transaction volume of € 3 million per month. Currently, five of 21 Belgian PIs operate under a waiver. Table 8 below lists all the PIs with a licence in Belgium in accordance with the different types of businesses they are involved in, and ranked according to their balance sheet size[3].

TABLE 8 CLASSIFICATION OF PIS WITH A LICENCE IN BELGIUM, RANKED ACCORDING TO THEIR BALANCE SHEET SIZE AND FOREIGN PIs WITH A REGISTERED BELGIAN BRANCH[1]

Card acquiring and Processing	Money Remittance	Direct Debit	Hybrid
	PIs		
Worldline	HomeSend	EPBF	Cofidis
Alpha Card	Travelex		FX4BIZ
B+S Payment Europe	MoneyTrans Payment Services		eDebex
Bank Card Company	Gold Commodities Forex		Oonex
Alpha Card Merchant Services	Belgian Money Corp		PAY-NXT
	PIs operating under a waiver		
Rent A Terminal	Money International		
Instele	Belmoney Transfert		
	Africash		
	Foreign PIs with Belgian branch		
	Munditransfers		BMCE EuroServices
			Santander CF Benelux

Source: NBB.
(1) Foreign PIs with a branch in Belgium are not ranked.

The electronic money sector is more limited, both in size and scope. At present, the Bank has 9 ELMIs under its prudential supervision, five of which are fully licensed and one is a foreign PI with an official and recognised Belgian branch. Also for ELMIs, a waiver regime exists for institutions that have an average outstanding value of electronic money below

(1) The Interchange Fee Regulation (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.) defines an acquirer as: "a payment service provider contracting with a payee to accept and process card-based payment transactions, which result in a transfer of funds to the payee".
(2) SEPA stands for Single Euro Payments Area and has fully harmonized the national payment instruments credit transfers and direct debits into European versions.
(3) The list can also be consulted on the website of the Bank at https://www.nbb.be/nl/financieel-toezicht/prudentieel-toezicht/toezichtsdomeinen/betalingsinstellingen-en-instellingen-5.

€ 5 million. Currently, three Belgian ELMIs have such a waiver. The total outstanding electronic money amounts to a relatively small amount, having reached its highest value of € 32 million in 2014. The main use of this electronicmoney is situated on internet platforms, pre-paid cards issued by credit card firms and gift cards. Proton was the largest Belgian electronic money solution (set up by the Belgian banks), processing transactions for more than € 308 million in its last year of active service in 2014. Table 9 below lists all the ELMIs with a licence in Belgium ranked according to their balance sheet size.

TABLE 9 LIST OF ELMIs WITH A LICENCE IN BELGIUM, RANKED ACCORDING TO THEIR BALANCE SHEET SIZE AND FOREIGN ELMI WITH A REGISTERED BELGIAN BRANCH

ELMIs
Imagor
Fimaser
Buy Way Personal Finance
Hi-Media Porte Monnaie Electronique (HPME)
Ingenico Financial Solutions
ELMIs operating under a waiver
Orange Belgium
RES Credit
Loyaltek Payment Systems
Foreign ELMI with Belgian branch
Ingenico Payment Services

Source : NBB.

Table 10 below gives an overview on the evolution of the PI and ELMI landscape within Belgium since 2011. It illustrates that there has been a gradual increase in licensed payment institutions, both those operating with a full licence and those with a waiver. On the electronic money side of the market, there has not been a major rise in the number of licences granted. This evolution illustrates the fact that new PIs are trying to gain a stronger foothold in the market, whereas for ELMIs fewer new initiatives were launched.

TABLE 10 EVOLUTION OF PIs AND ELMIs WITH A LICENCE IN BELGIUM AND WITH A REGISTERED BELGIAN BRANCH
(number of licenses, end of year)

	2011	2012	2013	2014	2015	2016
PIs						
Full Licence	9	10	12	11	12	16
Waiver Licence	0	0	2	4	5	5
Foreign PIs with Belgian branch	0	2	2	3	3	3
Total	**9**	**12**	**16**	**18**	**20**	**24**
ELMIs						
Full Licence	2	2	5	5	5	5
Waiver Licence	4	4	5	5	5	3
Foreign ELMIs with Belgian branch	0	0	0	1	1	1
Total	**6**	**6**	**10**	**11**	**11**	**9**

Source : NBB.

The future outlook for the industry remains mixed. On the one hand, there is still a lot of innovation within the payment services sector. For example, over the course of 2016, the Bank licensed institutions that combined multiple payment services in an innovative way, such as the offering of both mobile direct debit services and the acquiring of merchants. The implementation of PSD2 will stimulate this trend even further as new payment services are introduced and competition throughout the payment chain is encouraged. On the other hand, the popularity of electronic money is generally in decline. Among the drivers are the new mobile and digital payment solutions aiming to offer a more customer-friendly and more frictionless way of completing a transaction, both for the payer as payee. Nonetheless, innovation within the electronic money industry could continue to complement alternative business models in the payments landscape. Box 7 further elaborates on FinTech initiatives in payments.

PRUDENTIAL APPROACH

Since April 2011, 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, listed by Belgian law, to ensure the secure functioning and solvency of these institutions. The requirements with which institutions need to comply consist largely of the elements that were assessed throughout the authorisation process. For example, both before and after starting their activities, institutions should be able to provide evidence that they safeguard the funds received from clients. To enable the Bank to assess these ongoing requirements, institutions need to report on a quarterly basis a wide range of information, including financials and governance documents. In addition to this reporting requirement, institutions are legally required to appoint an accredited auditor to certify their balance sheet, account statements and regulatory reports. Important to note is that the institutions subject to a waiver regime have less stringent reporting requirements. For example, they do not need to submit their balance sheet on a quarterly basis. However, both types of institutions do have to notify the Bank if there are changes in the corporate governance structure.

SUPERVISORY PRIORITIES IN 2017

The Bank participates in the international work by the EBA (i.e. Task Force on Payment Services) delivering the necessary regulatory technical standards and guidelines to ensure a common European approach. In the transposition process, the Bank aims to minimise gold-plating[1], by respecting the EU rules, and wants to keep the regulatory burden low for both potential and existing institutions. Table 11 below gives an overview of the different regulatory technical standards and guidelines that are being developed within the EBA mandate under PSD2.

TABLE 11 OVERVIEW OF REGULATORY TECHNICAL STANDARDS AND GUIDELINES BEING DEVELOPED WITHIN THE EBA MANDATE UNDER PSD2

Regulatory Technical Standards
Passporting Notifications
Strong Authentication and Secure Communication Central Contact Points
EBA Register
Guidelines
Authorisation
PI Insurance for PSPs
Major Incidents Reporting
Complaints Procedure
Security Measures
Minimum Monetary Amount of the Professional Indemnity Insurance

Source : NBB.

(1) Gold-plating describes a process by which a Member State which has to transpose EU Directives into its national law, or has to implement EU legislation, uses the opportunity to impose additional requirements, obligations or standards on the addresses of its national law that go beyond the requirements or standards foreseen in the transposed EU legislation.

Box 7 – Fintech in payments: New technology, enablers, hurdles and potential impacts

The expansion of the Internet and associated new technologies turned innovation into an essential driver for the development of the payment industry. Customers started having new expectations for online and mobile payments, requiring adequate solutions to be developed. On the demand side, the widespread use of smartphones and the development of the Internet of Things (IoT) ushered in new needs for payment solutions, whereas on the supply side, these same developments triggered the setting up of innovative payment services and infrastructures. Moreover, the development of distributed ledger technologies or DLT, originally used by virtual currencies (e.g. the Blockchain of Bitcoin), opens up new possibilities for further innovations in these domains.

Increasingly, new technological solutions are being developed by non-banks, which become new entrants as payment service providers (PSPs) whereas so far banks had been the dominant PSPs. This technology-based phenomenon bringing innovations in the field of finance is often captured by the notion of FinTech. There is no universally accepted definition of this concept. It covers a wide variety of interacting financial actors, technologies and business models linked to an (expected) widespread acceleration of technological innovation used for the simplification and improvement in the provision of financial services. Among these services, payments represent a particularly active area.

RETAIL PAYMENTS SOLUTIONS

In the field of retail payments, FinTech covers a multitude of innovative solutions. These include for instance apps enabling mobile payments based on standard instruments such as debit and credit cards, credit transfers and direct debits; on the integration of multiple bank accounts on a single app, on the user-friendly and secure use of cards through biometrics and tokenisation, etc. The objective of these innovations is to meet customers' requests: user-friendly digital payment platforms based on superior design or directly integrated in the connected objects (IoT) as well as a faster processing of their payment transactions at a lower cost. FinTech uses new technologies to bring solutions to existing inefficiencies of current payment services.

DISTRIBUTED LEDGER TECHNOLOGIES

Born with Bitcoin less than a decade ago, the distributed ledger technologies may be promising for the future development of more efficient and less costly payment solutions which might no longer rely on a central entity for their operation but on a network of participants acting as node for the validation of transactions. This DLT technology, which is expected to be used not only in payments but in a wide range of domains, is currently being tested and assessed by different players around the world including central banks. Collaborative initiatives, such as Hyperledger[(1)] have emerged in order to commonly develop the technology and its potential applications. DLT also paves the way for the payment leg of smart contracts[(2)].

INTERNET OF THINGS (IOT)

The development of the IoT is likely to open up new needs for payment solutions. Physical items are increasingly being turned into connected objects that are able to interact with other objects in their environment. Examples of these innovations are refrigerators which are able to check their contents and directly order and pay for the missing items or cars which automatically manage the payment of the insurance premiums associated with their use (pay-per-use model). These payment interaction patterns require technology that enables frictionless payment,

(1) Hyperledger is an open-source collaborative effort created to advance cross-industry blockchain technologies. It is global collaboration, hosted by The Linux Foundation, including leaders in finance, banking, IoT, supply chain, manufacturing and technology.

(2) A smart contract permits users to include self-executing codes on the ledger to automate the fulfilment of contract terms

i.e. reduced complexity for the end user, low transaction costs and integrated payment solutions. DLT is currently investigated as a possible solution for IoT payments.

ENABLERS AND HURDLES

If technology is the main driver to the development of FinTech, other factors are likely to have a significant impact also. Among these factors, the legal environment will be a critical one. Conflicts with existing legislation or regulations, lack of legal harmonisation and legal uncertainties would probably have an adverse effect. However, when legislation stimulates the creation of new payment solutions and boosts competition, FinTech may be encouraged to play an even more significant role. This is what is likely to happen in the field of payments with the second Payment Services Directive (PSD2) which aims at improving the efficiency of the European retail payment services. PSD2 is expected to do so, in particular by bringing two new types of payment services, i.e. *payment initiation and account information*, into the regulatory scope. However, the most significant change brought by the PSD2 from a FinTech perspective is the requirement for banks and other account-holding institutions to enable those new categories of payment institutions to directly access the accounts of their customers. In other words, the Fintech companies will be able to develop their own payment solutions directly connected into the payment accounts of their customers.

Another factor influencing the development of FinTech innovations is the existing inter-PSP infrastructure (i.e. the retail payment systems) on which the new payment solutions often have to rely. Current retail payment systems generally provide end-of-day settlement and availability of funds on the beneficiary account on the next working day. The new needs in the fields of payments induce changes also at the level of the infrastructure and foster the development of new real-time retail payment systems for ensuring an immediate availability of funds to the payee, i.e. instant payments. Such instant payment systems will enable efficient and safe interbank settlement of the new payment solutions irrespective of whether they are offered by incumbent PSPs or by new actors. Several countries already have instant payment solutions in place.

FinTech initiatives are confronted with various hurdles. At technical level, the need for standardisation and interoperability with existing incumbent infrastructures as well as the integration readiness of the innovative services are still major challenges. From an investment perspective, significant resources are needed to build, bring to maturity and support FinTech solutions on a large scale in a short time. Regarding retail payments, the requirement of adoption by a critical mass could also be an impediment to the long-term success (and survival) of innovative solutions.

IMPACT ON THE FINANCIAL SECTOR

For the traditional PSPs, FinTech developments create additional competitive pressures, including from new non-bank entrants in the payment services area, which incites them to incorporate innovations in their payment services offering. On the other hand, FinTech developments bring along new opportunities for the existing, traditional PSPs, which often have the network advantage (innovations can be rolled out on a large scale over a large customer basis). While FinTech actors are usually new entrant start-ups, incumbent players have well understood the challenge ahead : they also develop their own FinTech innovations, cooperate with existing FinTech companies or buy those with promising development possibilities. As a result, the payment landscape evolves towards an increased complexity of the value chain and of the interactions between various actors with different status.

Additionally, the move to a real-time payment environment entails significant investment costs, not only to develop the real-time infrastructure but also to upgrade internal processing chains.

IMPACT ON CENTRAL BANKS

Central banks are also impacted by the new technological context brought by FinTech. As payment system operators, two issues are particularly relevant for them: the need to adapt to the real-time payment environment as well as the possible use of DLT in their own systems.

As regulator, central banks are confronted with a new fragmented landscape composed of multiple actors with various risk profiles and business models creating an increased need for monitoring interdependencies as well as technological developments and their use. The changeover to real-time settlement of payments also has the potential to make some risks more acute (e.g. credit risk and operational risk), as the reaction time to incidents is being shortened significantly.

3.3 Processors for retail payment instruments

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 oversight is currently based on cooperation, historic relationships with key market participants and the moral suasion exercised by the Bank. Incidents occurring at the dominant domestic payment processor over the last few years seriously impacted the proper functioning of card payment processing in Belgium. They demonstrate that soft-law-based oversight has, in this case, reached its limits and hence cannot always assure robust compliance with applicable oversight standards.

Subsequently, and in accordance with legal initiatives in the euro area, the Belgian Parliament has issued a new law[1] on processors of payment transactions that will significantly strengthen enforcement of the applicable oversight standards on all payment processors that are considered systemically relevant in the Belgian payment transactions market, regardless of where such processor has its registered office. Systemic relevance will be determined based on a threshold amount of Belgian payment transactions, calculated at the level of one particular payment scheme, for which a processor has rendered processing services.

BUSINESS ACTIVITY

Worldline SA/NV is the Belgian subsidiary of the Worldline group (Worldline e-payment services) which is, on its turn, a branch of the French company ATOS. The Worldline group offers payment solutions on a pan-European scale and has many subsidiaries and branches throughout Europe. Worldline SA/NV has systemic relevance from an oversight perspective since it has a systemically significant position in the processing of Belgian debit and credit card payments. New record peaks were registered in December 2016 with more than 8.42 million transactions processed in a single day (about 11.5 % more than the 7.55 million in December 2015), worth over € 630 million. The amounts aggregate all electronic payments, including online payments. At the end of 2016, Worldline SA/NV reported a 10 % increase in online payments, as well as a strong rise (+30 %) in electronic payments for small amounts below € 5.

On 27 September 2016, the Bank approved the contribution in kind of Worldline SA/NV's processing business unit in the Dutch automated clearing house[2] Equens SE (NL) in return for which it became a shareholder in Equens SE, which subsequently changed its name to equensWorldline SE. This merger was part of a pan-European merger plan between the French Worldline Group and Dutch ACH Equens SE whereby several Worldline entities (i.e. Belgium, Germany, France and Luxembourg) will jointly transfer their processing business units to Equens SE in return for an aggregate overall stake of roughly 63 % in Equens.

(1) Law of 24 March 2017 on the supervision of payment transactions processors, Belgian Official Gazette 24 April 2017.
(2) An automated clearing house is a retail payment system processing mass numbers of bulked payments in a fully automated way (mainly credit transfers and direct debits, sometimes also checks or card transactions).

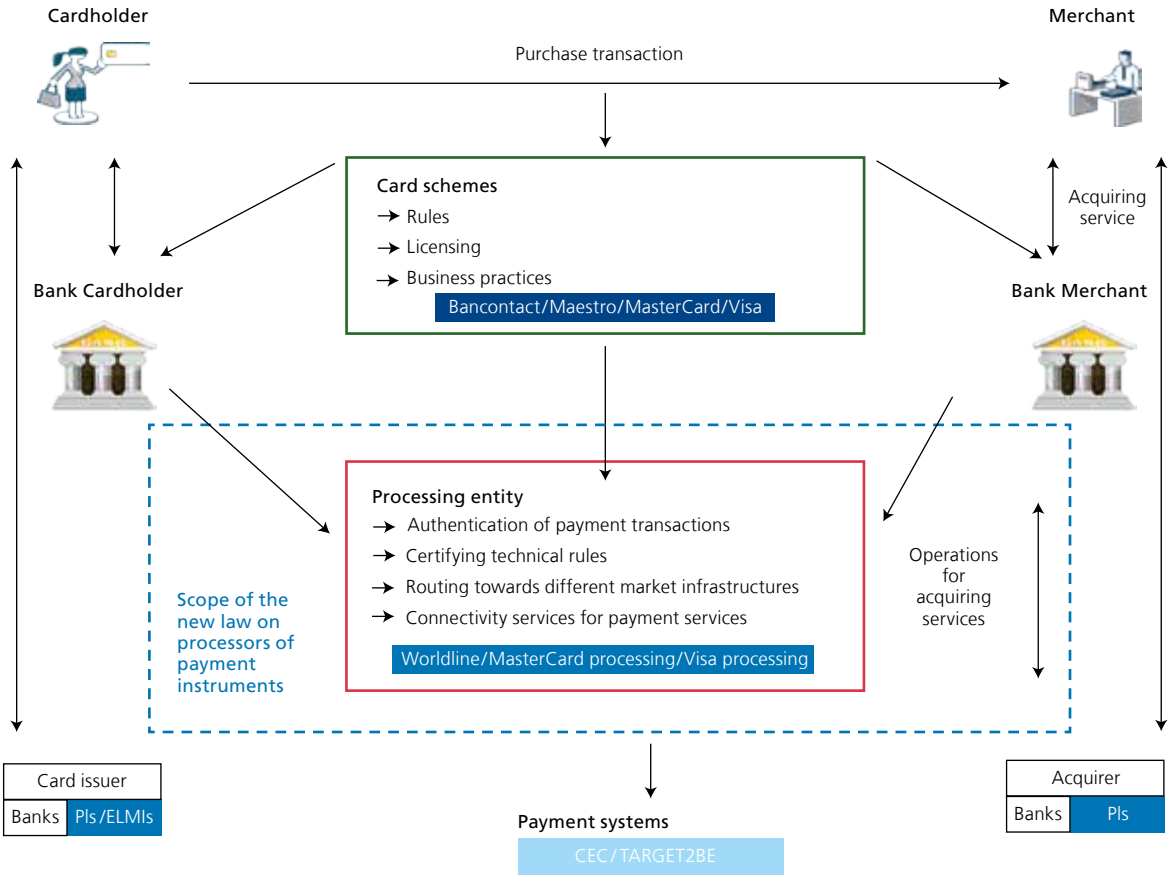
As a result of this merger, the platforms processing the overwhelming majority of Belgium's card payments became legally part of the newly merged company established in the Netherlands. As such, this posed challenges to the continued effectiveness of the Bank's proper oversight on this part of Worldline SA/NV's infrastructure. Accordingly, the Bank took several steps to seek assurance with regard to the ability to maintain and even strengthen its oversight on Worldline SA/NV's processing division.

PRUDENTIAL & OVERSIGHT APPROACH

The regulatory status of Worldline SA/NV is explained in box 8. The applicable oversight requirements of the new law on processors of payment transactions is inspired by 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). The new law creates an improved and more sharply defined legal framework for executing the oversight on systemically important payment processors in Belgium, allowing also – if and when necessary – the imposition of periodic penalty payments and administrative fines imposed by the Bank.

As illustrated in chart 15 below by way of example, the scope of the law (within the blue dotted border) is aimed at the processing activities that are not necessarily performed by the acquirer. Processing has been defined in a technology-neutral manner as the execution of technical processes necessary for and specifically aimed at the handling of a payment transaction, such as authentication, certification, routing and connectivity.

CHART 15 SCOPE OF THE NEW LAW ON PROCESSORS OF PAYMENT INSTRUMENTS



Source: NBB.

Box 8 – Worldline SA/NV subject to both oversight and prudential supervision

Worldline SA/NV has a systemically significant position in the Belgian card payments industry making the smooth functioning of nationwide card payments largely dependent on one company. It plays a critical role in most layers of the card payment market, including the provision of networks for POS (point of sale) and interbank ATM (automated teller machine) operations, acquiring activities on behalf of merchants for them to accept national and international debit and credit card payments, as well as the operation and management of domestic debit cards. The systemic importance of Worldline SA/NV from an oversight perspective stems from the services it renders to the public, merchants and financial institutions for whom any disruption in business is critical for the economy and from the end-to-end role it plays in the processing of payments. The increasing importance of card payments makes the role of Worldline SA/NV even more crucial for the Belgian economy and the risk even more critical than before. A default by the company would trigger a loss of confidence in crucial payment instruments and have adverse effects on the real economy, and therefore suitable alternatives have to be available to merchants for continuing their payments at any moment.

Worldline SA/NV has been subject to oversight by the Bank since the mid-1990s. Initially, this oversight was informal and focused on electronic money products. Reflecting the company's pivotal role in payments and the related concentration risk, oversight was formalised a few years later, its scope was extended over time and the practical oversight arrangements were laid down in Memoranda of Understanding.

The adoption of the Payment Services Directive in 2009 has put several payment services under a prudential supervisory regime, one of which is the acquiring business. Worldline SA/NV has the majority of Belgian merchants as its clients for acquiring their incoming card payments. As a major card payment acquirer for merchants, Worldline SA/NV obtained the status of payment institution (PI).

Since then, the regulatory status of Worldline SA/NV is twofold: on the one hand, prudential supervision by the Bank covering its acquiring business and, on the other hand, oversight by the Bank because of its card payment processing activities that are crucial for the Belgian card payments business.

SUPERVISORY PRIORITIES IN 2017

The Bank will start implementation of the new legal framework for processors of retail payment instruments. Where applicable and as stipulated in the new law, regulations will be prepared to further detail the Law's requirements on the level of, for example, due diligence, notifications of incidents and (un)availability of the system.

The Bank will also establish an oversight Memorandum of Understanding with De Nederlandsche Bank with regard to equensWorldline SE.

3.4 Card payment schemes

In the euro area, the sound and safe functioning of card payment schemes (CPSs) is monitored by central bank oversight according to the following allocation of tasks.

The ECB, in cooperation with the Eurosystem national central banks (NCBs), is in charge of the standard-setting process, as well as determining when specific assessment rounds have to be undertaken in each jurisdiction. The Eurosystem oversight framework for CPSs dates from 2008[1]. An amended guide for the assessment of CPSs against the oversight

(1) ECB (2008), Oversight framework for card payment schemes – standards, (https://www.ecb.europa.eu/pub/pdf/other/oversightfwcardpaymentsss200801en.pdf).

standards was published in February 2015[1]. Over and above the Eurosystem requirements, NCBs have the discretion to apply any additional measures they deem relevant for the CPS under their oversight.

The monitoring of ongoing compliance, through frequent interactions with the CPSs, is the job of the NCB from the jurisdiction where the CPS is legally established. The Belgian domestic CPS, Bancontact, is subject to oversight by the Bank. In this case, the results of an assessment of its compliance with the Eurosystem CPS standards are peer reviewed at the Eurosystem level.

For CPSs with cross-border activities, assessment rounds are organised by recourse to an assessment group, made up of representatives of NCBs having a legitimate interest in the sound functioning of the CPS. The conduct and coordination of these assessment groups are in principle the responsibility of the NCB from the jurisdiction where the international CPS is legally established. This is the case for Mastercard Europe (MCE), established in Belgium, and for which the Bank ensures the role of overseer within the Eurosystem framework.

CHANGES IN REGULATORY FRAMEWORK

EU Regulation 2015/751 on interchange fees for card-based payment transactions (IFR)[2] contains (i) the definition of a cap for the interchange fees applicable to payment transactions by means of debit or credit cards (Article 4), (ii) the separation to be put in place between payment card scheme governance activities and processing activities (Article 7.1 a), (iii) several measures granting more autonomy to merchants regarding the choice of payment instruments they wish to be used by their clients.

The separation to be put in place in accordance with IFR between payment card scheme governance activities (i.e. rules, licensing, business practices) and processing activities (i.e. the performance of payment transaction processing services in terms of the actions required 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) is depicted in chart 15 above (payment card scheme governance and processing activities framed by respectively the green and red straight lines). The unbundling of the scheme and processing activities (when performed within the same legal entity) will result in the setting up of Chinese walls inside that same legal entity in order to put the processing business unit on an equal footing with external processing firms as regards the scheme activities.

According to the European authorities, the separation of payment card scheme governance and processing activities should allow all entities and firms offering processing services to compete for customers of the schemes. As the cost of processing is a significant part of the total cost of card acceptance, it is important for this part of the value chain to be opened to effective competition. On the basis of the separation of scheme and infrastructure, card schemes and processing entities, even if present inside the same legal entity, should be independent in terms of accounting, organisation and decision-making process. They should not discriminate, for instance by providing each other with preferential treatment or privileged information which is not available to their competitors on their respective market segment. In such a new context, no more privileged exchanges of information will be allowed between the scheme and processing business units of a single legal entity.

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, which has been designated as overseer of MCE within the Eurosystem framework to ensure the compliance of MCE with Article 7, requiring separation between card payments schemes and card processors[3].

In 2016, the Bank integrated the EBA guidelines on the security of internet payments into its prudential supervision framework[4] which are also relevant for CPSs because the latter have to provide their customers (issuers and acquirers)

(1) ECB (2015), Guide for the assessment of card payment schemes against the oversight standards, (https://www.ecb.europa.eu/pub/pdf/other/guideassessmentcpsagainstoversightstandards201502.en.pdf?499089f7f3aab273925ef6d80767b4a5). See also *Prudential and oversight approach* in this section.

(2) Regulation (EU) 2015/751 of the European Parliament and of the Council of 29 April 2015 on interchange fees for card-based payment transactions, OJ. 19 May 2015, L. 123, 1-15 (http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R0751&from=en).

(3) According to the Law of 1 December 2016 enforcing Regulation (EU) 2015/751 of the European Parliament and of the Council of 29 April 2015 on interchange fees for card-based payment transactions, Belgian Official Gazette 15 December 2016, 86.578.

(4) NBB Circular Letter 2016_29, 25 May 2016 (https://www.nbb.be/doc/cp/fr/2016/20160525_nbb_2016_29.pdf).

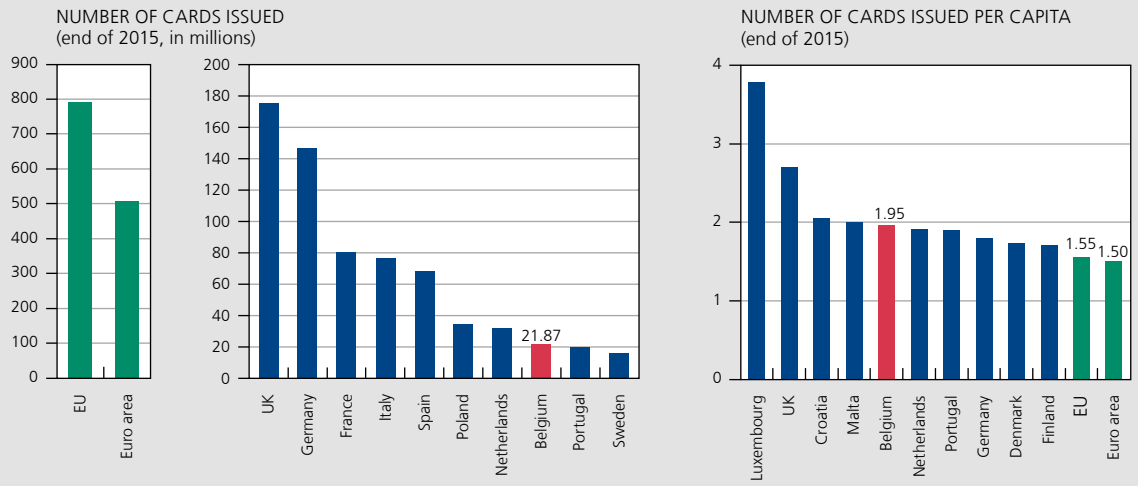
with all the necessary elements for them to comply with the guidelines mentioned above. On the prudential side, the new guidelines are not considered as a major evolution in Belgium as a CBFA 2009 Circular[1] had already submitted PSPs in retail payments established in Belgium to the vast majority of the EBA guidelines referred to. For CPSs – thus from an oversight perspective – a number of features of the new EBA guidelines on the security of internet payments have been included by the Eurosystem in its oversight framework applicable to CPSs, specifically the ones related to strong customer authentication.

BUSINESS ACTIVITY

The following charts present global card payment statistics (debit, delayed debit and credit functions) for all brands. For Belgium, it includes the regular Belgian payment cards which are, in most cases co-branded with the Bancontact and Maestro payment schemes, allowing card holders to make card payments, respectively on the Belgian market and cross border. The use of cards in Belgium is compared with that in the EU top 10 countries, as well as the euro area or EU as a whole[2].

Based on available 2015 data, chart 16 (left-hand panel) shows that almost 22 million cards were issued in Belgium by resident payment service providers (PSPs) (i.e. banks, PIs, ELMIs). With 1.95 cards per person, Belgium pertains to the EU top 5 in terms of number of cards issued per capita (chart 16, right-hand panel). The number of cards issued per capita in Belgium is higher than the average number for the euro area (1.50) and the EU (1.55).

CHART 16 CARDS ISSUED BY RESIDENT PAYMENT SERVICE PROVIDERS – TOP 10 EU COUNTRY COMPARISON[1]



Source: ECB.
(1) Cards with a cash function

Chart 17 provides 2015 data on payment transactions per card (top panel) and card payment transactions per capita (bottom panel).

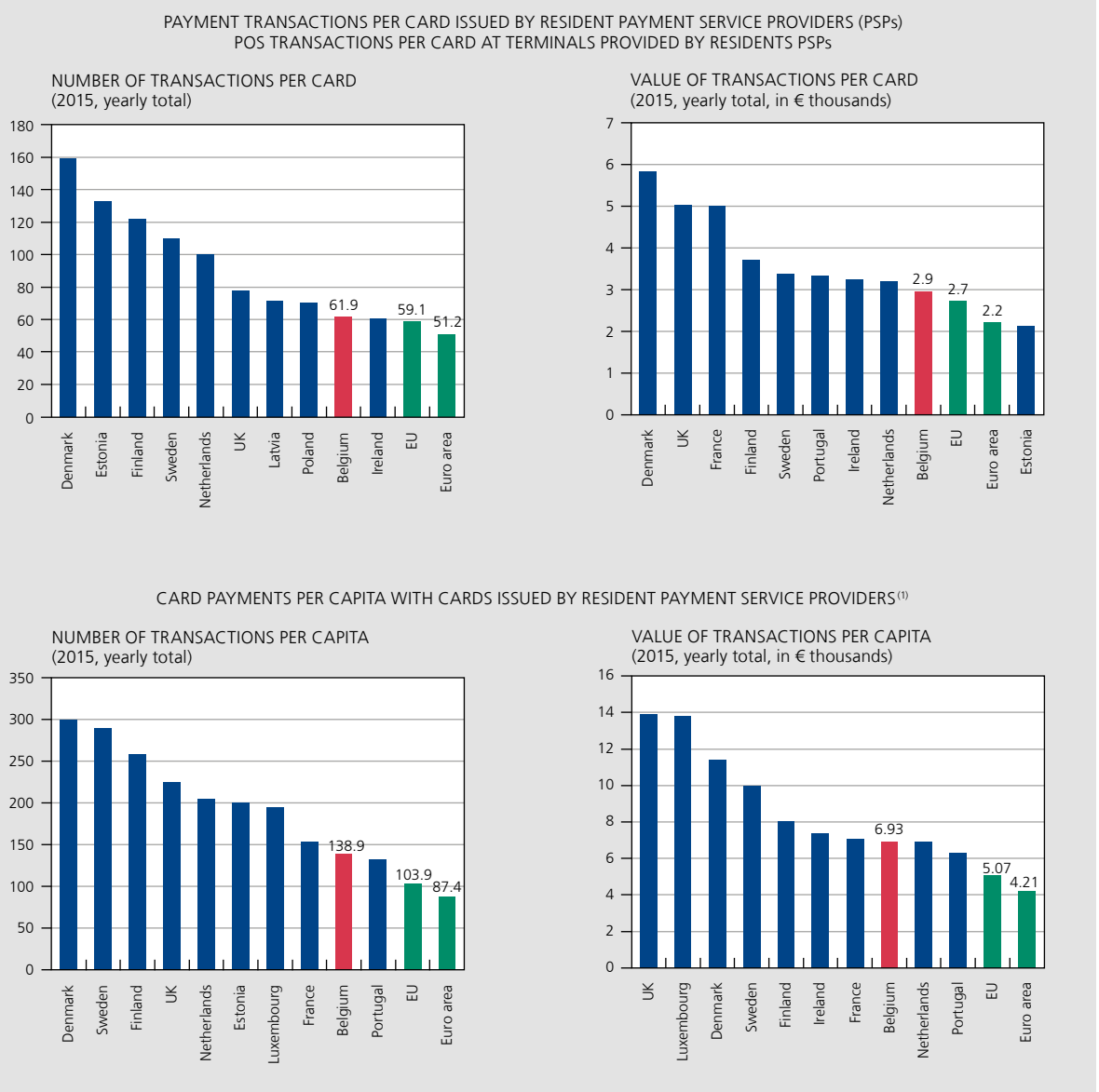
In Belgium, on average, close to 62 payment transactions per card issued by resident PSPs are processed at retail locations (at point of sale (POS) terminals provided by resident PSPs) on a yearly basis. The number of payment transactions per

(1) CBFA Circular Letter 2009_17 Financial services via internet: prudential requirements and its annex "Sound practices regarding the risk management of the security of internet transactions", 7 April 2009 (https://www.nbb.be/en/articles/circular-cbfa200917-financial-services-internet-prudential-requirements).
(2) CPS statistics collected for oversight purposes, under the auspices of the Eurosystem, are subject to strict confidentiality rules due to their commercial sensitivity. This prevents disclosure by the national central banks or the ECB that would enable the identification of any individual CPS.

card at POS terminals in Belgium is well above the average for the euro area and the EU (respectively about 51.2 and 59.1). In value terms, POS payment transactions processed per card for a full year in Belgium represent € 2 948. Again, the activity per card is well above the average for the euro area and the EU as a whole (respectively € 2 212 and 2 729).

Per capita, and on a yearly basis, close to 140 payment transactions are processed via cards issued by resident PSPs in Belgium, representing close to € 7 000 in value terms. Average card transactions per capita in Belgium are higher than those in the euro area and the EU as a whole, both in number (respectively about 87.4 and 103.9) and value (respectively about € 4 210 and 5 070).

CHART 17 CARD PAYMENT TRANSACTIONS – TOP 10 EU COUNTRY COMPARISON



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

OVERSIGHT APPROACH

A structured oversight of CPSs' performance is in place in order to ensure the public's trust in the stable and sound functioning of payment systems and instruments in the broad sense.

The Eurosystem oversight framework for CPSs 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 2017) 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. Indeed, due to their central position in processing card payments, it is crucial that CPSs' modus operandi 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 state-of-the-art practices and existing standards.

This gap assessment was carried out through a cooperative assessment group with regard to MCE (and the other international CPSs), while the Bank undertook the analysis on a solo basis vis-à-vis Bancontact (the Belgian domestic CPS) to be finalised by a peer review process at Eurosystem level.

The National Bank of Ukraine (NBU) approached the Bank because of the systemic importance of the Mastercard payment scheme in its country. In accordance with the international cooperation principles governing oversight, and in order to avoid redundant requests from several authorities to the same CPS, the Bank concluded in mid-2016 an Memorandum of Understanding with the NBU on sharing information for the oversight of MCE. The Bank has already entered into a similar partnership with the central bank of the Russian Federation since May 2013. In addition to those countries, MCE is also considered of systemic relevance for the authorities of other European countries, including the Netherlands, where it has replaced the domestic CPS. In such cases, the exchange of information is organised by the cooperative oversight at Eurosystem level.

OVERSIGHT PRIORITIES IN 2017

The main oversight priorities for CPSs in 2017 are threefold. Firstly, setting up a cooperation mechanism for monitoring the correct implementation of the IFR where the focus will be on the requirement to separate payment card scheme governance activities and processing activities. Secondly, finalisation of the gap assessment of the CPS sector based on the updated Eurosystem oversight framework integrating requirements relating to strong customer authentication. Finally, further analysis of cyber risks and the adequacy of the cyber resilience framework of the CPSs established in Belgium.

4. SWIFT

The Society for Worldwide Interbank Financial Telecommunication (SWIFT) is a limited liability cooperative company registered in Belgium that provides messaging services to both financial institutions and market infrastructures. These customer types are characterized 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.

Nearly half of SWIFT messaging activity is related to the exchange of payment information between banks involved in correspondent banking arrangements. SWIFT provides messaging and connectivity services to a large number of market infrastructures, e.g. in the context of large-value payment systems (section 3.1) to help limit settlement risks in the interbank payment process. Messaging services are also being provided to CLS Bank (see box 6) that eliminates settlement risk for foreign exchange transactions between currencies.

Additionally, the cooperative is an active promotor of structural cooperation within the payment and settlement industry. In collaboration with its members, SWIFT focuses on refining existing message types and defining message standards for new transaction types or other financial information needs. Recently, SWIFT has also been focusing on improving the cyber resilience of its customers by supporting them in securing their local infrastructure.

Although SWIFT is neither a payment system nor a settlement system, a large number of systemically important systems depend on it for their daily messaging, so that SWIFT – as a critical service provider (CSP) to these systems – is itself of systemic importance (see chart 18 below). For these reasons, the central banks agreed to make SWIFT subject to cooperative central bank oversight (see box 9). By jointly interacting with SWIFT and formulating joint recommendations vis-à-vis SWIFT, central banks aim to increase the efficiency of their interactions with SWIFT as well as the effectiveness of the SWIFT actions taken in reaction to their recommendations.

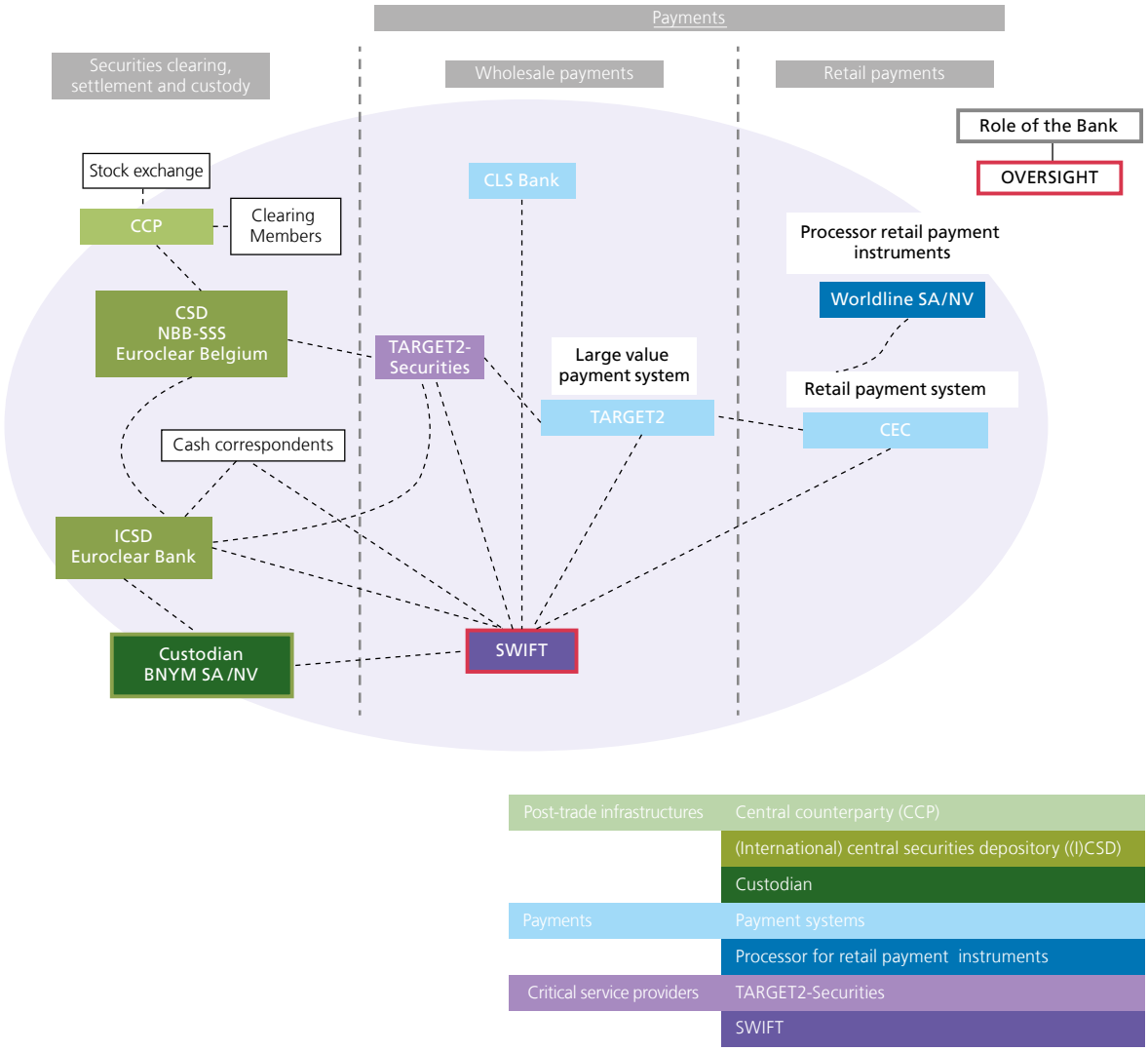
SPECIFIC ATTENTION POINTS IN THE OVERSIGHT FRAMEWORK

While the regulatory framework for SWIFT remains unchanged, the overseers have identified the Customer Security Programme as an important area within scope of the oversight arrangement. The development and roll-out of this programme exposes both SWIFT and its customers to specific risks, while at the same time a successful adherence to the Customer Security Programme by SWIFT's participants would increase overall cyber resilience.

Recent cyber incidents at SWIFT participants have indicated the importance of effective cyber security measures at all entities involved in the processing of financial transactions, i.e. end-to-end security in the transaction chain. SWIFT informed the overseers and its customers of these cyber incidents and indicated it obtained reasonable assurance that neither the network nor the operations had been compromised. As attackers were able to exploit weaknesses in the IT environment of SWIFT's customers, a need for reiterating the importance of end-to-end security in the transaction chain was identified.

SWIFT's Customer Security Programme is dedicated to support its customers in reinforcing the cyber security measures of their SWIFT infrastructure and adds an important security framework for other financial institutions and market

CHART 18 SWIFT AS CSP TO THE FINANCIAL INDUSTRY AND THE BANK'S OVERSIGHT ROLE



infrastructures. It is designed around three mutually reinforcing areas: secure and protect; prevent and detect; and share and prepare.

The first area, secure and protect, focuses on improving the cyber security posture of SWIFT's customers. A core set of mandatory security controls that aim at enhancing the security baselines is provided. Customers will be asked to attest their compliance. Given the potential impact on the financial industry, the overseers continue to review and assess the effectiveness of the proposed measures. Similarly, the strengthening of the security requirements for customer-managed software is being followed up.

The second area, prevent and detect, deals with the development and promotion of detection mechanisms at the message sender's side, as well as the active management of counterparty relationships (e.g. ensuring that you can only receive messages from trusted parties). These applications fall in the traditional oversight scope.

The third area, share and prepare, centres on deepening SWIFT's cyber security forensics and analysis capabilities so as to develop intelligence on SWIFT-related events.

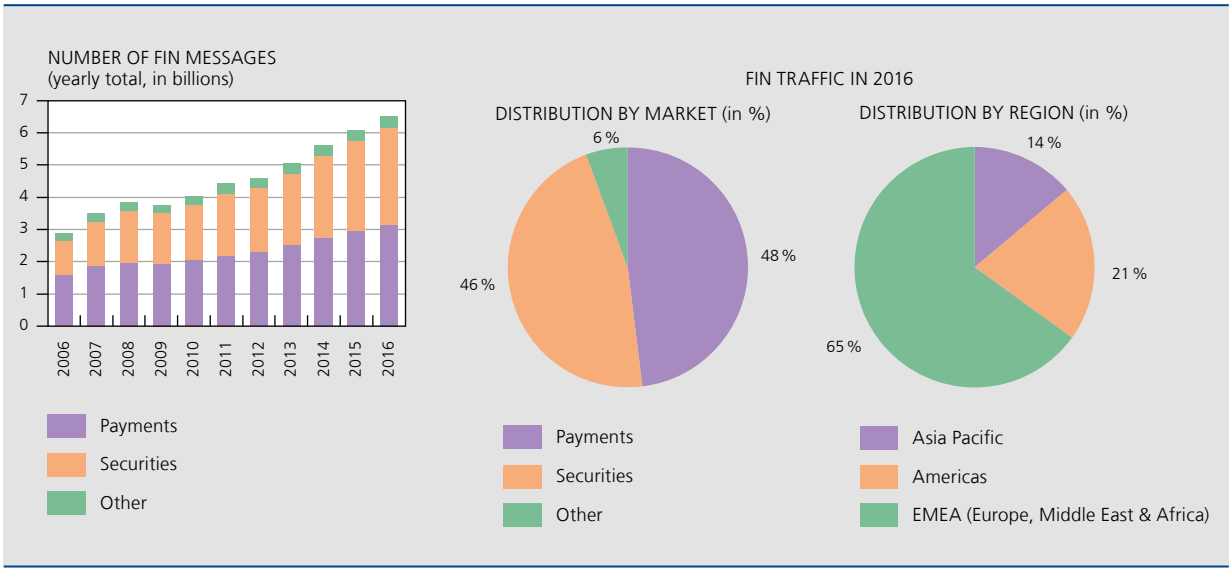
In June 2016, the NBB issued on its website a joint statement of the SWIFT overseers on reinforcing cyber resilience of the financial ecosystem[1]. The document expresses the common understanding of the importance of the cyber security arrangements of SWIFT's users in the overall cyber resilience of the financial system.

BUSINESS ACTIVITY

SWIFT is owned and controlled by its members. It has an ongoing dialogue with its users 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. Each member has a number of shares proportional to its usage of SWIFT's message transmission services. Every three years, a share reallocation is implemented to reflect changes in each member's use of SWIFT. Countries or country constituencies can recommend directors to the board according to the number of shares owned by all members in each country.

FIN is SWIFT's core messaging service for exchanging financial messages. Total FIN traffic volume in 2016 reached 6.5 billion messages (+ 6.5 % compared to previous year), i.e. about 25.8 million messages per day. While large-value payment systems have contributed significantly to the growth in messaging via SWIFT in the previous decade, the growth in securities traffic has been even greater : securities messaging grew from one-third of SWIFT's total traffic to nearly half of the traffic (chart 19, left panel). These messages flow between participants in stock exchanges, payment systems, (I)CSDs and CCPs, as depicted in chart 18. SWIFT FIN traffic in 2016 was about 48 % related to payments and 46 % to securities messaging, while the main part of the traffic originated from EMEA members (65 %), before those from the Americas region (21 %) (chart 19, right panel).

CHART 19 SWIFT FIN ACTIVITY



Source : SWIFT.

OVERSIGHT APPROACH

SWIFT's messaging activities for payment and securities settlement infrastructures has been recognised as a significant factor in the safety and efficiency of payment and securities settlement systems. The Bank acts as the lead overseer – SWIFT is incorporated in Belgium – and conducts the oversight in direct cooperation with the other G10 central banks.

(1) https://www.nbb.be/doc/cp/eng/publications/swiftoversightforum.pdf.

In 2012, the arrangement was complemented with a structure comprising the senior overseers form the G20 countries, which discusses oversight policy and results. A complete overview of the oversight set-up can be found in box 9.

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 case of major contingency situations related to SWIFT.

The overseers' focus on SWIFT's management of operational risks is articulated into five High Level Expectations (HLEs) that focus on risk management (see box 10). These HLEs are providing SWIFT and overseers with a common language, a framework within which discussions can be held. These expectations vis-à-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[1].

(1) CPMI-IOSCO (2012), Principles for financial market infrastructures, BIS (http://www.bis.org/publ/cpss101a.pdf).

SWIFT provides the overseers with a regular self-assessment report regarding its compliance with the HLEs. This compliance assessment does not reflect the overseers' opinion, but is one of the starting points for the identification and further analysis of risk drivers at SWIFT.

Cyber and information security, a major driver for operational risk at SWIFT, has been a standing topic in the oversight of SWIFT. Based on cyber threat and strategy discussions with the security experts of SWIFT, the overseers conduct a risk assessment and identify the review priorities. In 2016, the overseers focused on the processes for cyber event detection, monitoring and response, taking also into account the use and creation of cyber intelligence at SWIFT. The interaction with and communication strategies for international Information Sharing and Analysis Centres (ISACs) has been analysed. Yearly, the overseers also review the processes for business continuity and disaster recovery.

The results of logical intrusion tests (with a specific testing scope such as one particular system or interface) and red team tests (i.e. expert team that is not bound by a testing scope) are extensively reviewed by the overseers and discussed with the management and security experts, and the remediation plans are reviewed. Overseers also followed up on the scale-up of the red teams and the available security skill mix. Deep-dives have been conducted towards the processes for assessing, managing and patching vulnerabilities, as well as the interaction with third-party vendors. Yearly, the overseers have the opportunity to challenge the external security auditor and its findings.

Overseers are also seeking to obtain reasonable assurance that entry points to the SWIFT network that are beyond its control are well-managed. Due diligence criteria and assessments for consumers, shared infrastructure providers and vendors of interface software are being monitored. In this context, the overseers have identified the Customer Security Programme that reaches well beyond SWIFT as a long-term area of oversight attention.

Additionally, SWIFT regularly presents its long-term technology strategic thinking and concrete platform investments. Major projects include cyber security investments, technological renewals and projects to improve efficiency and effectiveness for the customers such as the Global Payment Innovation Initiative[1]. The strategic proposals are challenged and tested against the overseers' requirements for security with special attention for information confidentiality, integrity and availability.

Overseers conduct regular evaluations of the effectiveness of the different lines of defence and governance structures, for daily operations, long-term strategies and specific projects (e.g. Customer Security Programme). Specific attention goes to the development and implementation of the enterprise risk management roadmap and the recurring assessment of extreme risks and recovery plans.

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

(1) https://www.swift.com/our-solutions/global-financial-messaging/payments-cash-management/swift-gpi.

Box 10 – High Level Expectations (HLEs) for (the oversight of) SWIFT

HLE 1. RISK IDENTIFICATION AND MANAGEMENT

SWIFT IS EXPECTED TO IDENTIFY AND MANAGE RELEVANT OPERATIONAL AND FINANCIAL RISKS TO ITS CRITICAL SERVICES AND ENSURE THAT ITS RISK MANAGEMENT PROCESSES ARE EFFECTIVE.

To help determine the extent to which this expectation is met, overseers review – and SWIFT should provide timely access to – all information they judge relevant regarding the following:

– the processes for risk identification and management, documenting the identified risks, the controls implemented to manage those risks, and the decisions made to accept risks;
– the processes for reviewing previously accepted risks in the light of new information;
– SWIFT's structures and processes set up to manage risks effectively;
– the extent to which SWIFT provides for effective assessments of risks and risk management processes through board of directors' oversight and independent internal and external audits.
– the extent to which the internal audit:
    - adheres to the principles of a professional organisation, such as the Institute of Internal Auditors, which govern audit practice and behaviour;
    - independently assesses inherent risks, as well as the design and effectiveness of risk management processes and internal controls to mitigate risks; and
    - clearly communicates its assessments to relevant Board members and has direct and immediate access to the chair of the Board's Audit & Finance Committee.
– how risks are monitored and managed in various domains, including at least the following:
    - dependency on third parties;
    - legal and regulatory requirements pertaining to SWIFT's corporate organisation and conduct;
    - relationships with customers;
    - strategic decisions with an impact on the longer-term continuity of the critical services;
    - risks related to information security, reliability and resilience, and technology planning, which are further elaborated on in HLEs 2, 3 and 4.

HLE 2. INFORMATION SECURITY

SWIFT IS EXPECTED TO IMPLEMENT APPROPRIATE POLICIES AND PROCEDURES, AND DEVOTE SUFFICIENT RESOURCES, TO ENSURE THE CONFIDENTIALITY AND INTEGRITY OF INFORMATION AND THE AVAILABILITY OF ITS CRITICAL SERVICES.

To help determine the extent to which this expectation is met, overseers review – and SWIFT should provide timely access to – all information they judge relevant regarding the following:
– information security policy or framework, and any processes and procedures for monitoring compliance;
– capacity planning;
– change management practices; and
– assessments of the implications of changes to SWIFT's operations on information security.

HLE 3. RELIABILITY AND RESILIENCE

COMMENSURATE WITH ITS ROLE IN THE GLOBAL FINANCIAL SYSTEM, SWIFT IS EXPECTED TO IMPLEMENT APPROPRIATE POLICIES AND PROCEDURES, AND DEVOTE SUFFICIENT RESOURCES, TO ENSURE THAT ITS CRITICAL SERVICES ARE AVAILABLE, RELIABLE AND RESILIENT AND THAT BUSINESS CONTINUITY MANAGEMENT AND DISASTER RECOVERY PLANS SUPPORT THE TIMELY RESUMPTION OF ITS CRITICAL SERVICES IN THE EVENT OF AN OUTAGE.

To help determine the extent to which this expectation is met, overseers review – and SWIFT should provide timely access to – all information they judge relevant regarding the following:
– business continuity and disaster recovery objectives, strategies and plans, including the extent to which they address the risk of a major operational disruption;
– business continuity and disaster-testing plans, procedures, and results, including the extent to which SWIFT facilitates periodic testing with customers; and
– procedures and processes to record, report, and analyse all operational incidents.

HLE 4. TECHNOLOGY PLANNING

SWIFT IS EXPECTED TO HAVE IN PLACE ROBUST METHODS TO PLAN FOR THE ENTIRE LIFECYCLE OF THE USE OF TECHNOLOGIES AND THE SELECTION OF TECHNOLOGICAL STANDARDS.

To help determine the extent to which this expectation is met, overseers review – and SWIFT should provide timely access to – all information they judge relevant regarding the following:

- IT strategic plans and processes for maintaining and updating those plans;
- the extent to which technology decisions balance the near-term needs of individual service enhancements with the planned long-term technology path for the service;
- assessments of the maturity of technologies being evaluated for introduction into the SWIFT environment;
- standards selection process when deploying and managing a service, and the standards maintenance and review process over time; and
- processes to ensure that design choices consider information security risks for the user community.

HLE 5. COMMUNICATION WITH USERS

SWIFT IS EXPECTED TO BE TRANSPARENT TO ITS USERS AND PROVIDE THEM INFORMATION THAT IS SUFFICIENT TO ENABLE USERS TO UNDERSTAND WELL THEIR ROLE AND RESPONSIBILITIES IN MANAGING RISKS RELATED TO THEIR USE OF SWIFT.

To help determine the extent to which this expectation is met, overseers review – and SWIFT should provide timely access to – all information they judge relevant regarding the following:

- customer communication procedures and processes to inform users of:
    - their role and responsibilities, including in the case of disruptions to SWIFT's critical services (crisis communication);
    - SWIFT's management processes, controls, and independent reviews of the effectiveness of these processes and controls; and
    - identified weaknesses (absent or non-performing controls) if users need such information to manage risks related to their use of SWIFT;
- techniques SWIFT uses to be informed by users of operational risks on the user side that could potentially affect its own operations, or, alternatively, techniques SWIFT uses to prevent any such user impact on its operations; and
- consultative mechanisms to ensure that SWIFT's technology choices that affect user operations are acceptable to the principal users of the critical services.

OVERSIGHT PRIORITIES IN 2017

The primary oversight focus for 2017 is on the adequacy of SWIFT's cyber strategy for the infrastructure, network and operations under its responsibility. In addition to a review of the investments in cyber security measures, a series of in-depth reviews are foreseen such as the hardening of the SWIFT tools, the identity and access management measures and the security culture.

In line with the need for a more holistic approach to cyber security, the overseers will continue to follow-up on the roll-out of SWIFT's Customer Security Programme. Part of this follow-up will be an assessment of the adequacy of the mandatory security controls and the transparency of communications with users on cyber security events and responsibilities.

Additionally, the overseers have a selection of standing topics. Firstly, the overseers continuously assess the effectiveness of the three lines of defence, i.e. line management, risk management and internal audit. Targeted oversight analyses should provide insight in the strategic infrastructure decisions, as well as the functioning of the enterprise risk management processes (e.g. risk identification, documentation and management). A selection of internal audit reports

will be reviewed to obtain reasonable assurance on the independence and objectivity of the internal auditor. Objective and independent audits provide the overseers with important evidence on the risk mitigation capabilities and security posture of SWIFT. Additionally, the findings, if any, of the external security auditor will be analysed and potential remediation discussed.

Secondly, the overseers start from the analysis of the risk of major operational disruption, to analyse and evaluate the business continuity processes, disaster recovery objectives and strategies. In this context, the overseers will assess the processes and strategies against the requirements elaborated in the new CPMI-IOSCO guidance on cyber resilience[1]. Special attention will go to the proposals for the 2 hour recovery time objective specified in the guidance.

Thirdly, risk-based assessments for strategic IT decisions and technology renewal are being conducted, as well as a review of the vendor due diligence processes and incident response integration. These risk assessments explicitly take into account the implications for the confidentiality, integrity and availability of information for the infrastructure, network and operations under control of SWIFT and of its users.

Fourthly, the overseers will judge the communication procedures and processes to inform users of their roles and responsibilities. In the light of the recent cyber incidents and the importance of the distribution of actionable cyber threat intelligence, the overseers decided to analyse the procedures and processes for communicating weaknesses identified at SWIFT or one of its customers to SWIFT's community.

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. Overseers will seek assurance that SWIFT has sufficient attention for the security features of its interfaces when further developing them in line with the evolving cyber threat evolutions. Additionally, the overseers will focus on the security requirements (and their differentiation) for the different options to access SWIFT services, this includes an analysis of the due diligence criteria, processes and results for third-party interfaces and shared infrastructure providers.

(1) CPMI-IOSCO (2016), Guidance on cyber resilience for financial market infrastructures, BIS (http://www.bis.org/cpmi/publ/d146.pdf).

Specific Themes

Cyber security in financial market infrastructures

Thomas Provoost

Cyber crime has seen an exponential rise over the last decade and a significant part targeted the financial sector in particular. During the course of 2016 alone, the vulnerability of information assets and the importance of safeguarding the confidentiality, integrity and availability of these assets have been made clear to all parties in the financial ecosystem (see box 1 on the most prominent cyber events revealed in 2016). These threats to information flows and the infrastructure that stores and processes them are central in the confrontation between cyber attackers and the institutions that find themselves defending their systems. This article takes a look at the attributes and channels the offensive side is targeting, and, at the defensive side, how strategies such as testing and information-sharing can be leveraged in creating a sustainable long-term approach by and for financial institutions and the ecosystem in which they work. While all participants in the financial community are facing roughly similar challenges stemming from cyber threats, some particularities for financial market infrastructures (FMIs) will be covered, since these are often at the heart of today's hyperconnected ecosystem.

Cyber criminals[1] seek out targets that yield them the highest expected pay-off : those that show low resistance to intrusion and extraction of value (high chance of success), or where high values can be extracted (big pay-out). In contrast to 'traditional', physical-world crime, the risk of being caught plays a much smaller role in this, not least since cyber space offers many opportunities to act across jurisdictional borders. Furthermore, the anonymity and jurisdiction-transcending nature of cyberspace has given rise to digital marketplaces where an economy of illicit information, tools and services is flourishing (often referred to as the "dark web"). The challenging nature of regulating and enforcing these types of criminal activity confounds the construction of adequate defence measures, since dissuasion by threat of incrimination is an implicit component of any institution's physical defences. But properly-functioning national law enforcement can not easily be transposed into the virtual world, and broad, actionable international cooperation as a necessity for a suitable crime deterrent is only to be encouraged.

The fact that more valuable channels are being targeted could be observed from a growing focus on the high-value transaction chain (bank back offices and interbank payments) as opposed to targeting retail customers (bank accounts). The Bank of Bangladesh case in February 2016 is the most notable instance. But next to being a force in choosing targets, the NBB (the Bank) has noticed that this optimisation of expected pay-off by criminals is also influencing what attribute of information[2] is sought to be compromised. There has been more pressure on the integrity element of data, as cyber criminals are finding ways to fraudulently create or alter rogue payments. This is happening in both the retail and the large-value domain, as evidenced by the recent Tesco Bank (UK) and Bank of Bangladesh heists respectively.

(1) For the purposes of this article, the generic term 'criminals' is used to designate the parties that are on the offensive side. This includes criminal activities such as theft of information or funds, but also refers to more advanced persistent threats such as cyber terrorism and nation-state attacks. These do not seek financial gain *per* se, but their objective lies in obtaining or disrupting information flows. This does not impact the further analyses of this text.

(2) To remind the reader, information has three critical characteristics (or attributes) that need to be maintained in any system : **confidentiality** (no disclosure of information to unauthorised individuals, entities, or processes), **integrity** (assurance of accuracy and completeness of data over its entire life cycle), and **availability** (accessibility of information when needed).

Nevertheless, the characteristics of availability and confidentiality remain under heavy fire, as seen by respectively the 21 October 2016 Internet of Things-powered DDoS attack ("Mirai") and the data theft at Yahoo widely covered in 2016 (see box 1).

Box 1 – The most prominent cyber events of 2016 (1)

Bank of Bangladesh (Bangladesh): In February, cyber criminals hacked into the systems of the Bangladesh central bank and, by compromising the local IT environment, attempted to make several fraudulent transfers. These added up to a total value of $ 951 million. While many of the payments were blocked, $ 81 million was still funnelled out to accounts in the Philippines and diverted to casinos there. Most of those funds are still missing.

Democratic National Committee (USA): In June, reports were made public of two separate breaches in the computer network of this American political organisation. Hacker groups gained access to the entire system, including research databases and emails (which were leaked to the public in July).

Yahoo ! (USA and global impact): In September, this internet company reported the compromise of more than 500 million of its users' names, e-mail addresses, birthdates, phone numbers, and passwords in a breach in 2014. An investigation was triggered by the discovery of a significant chunk of this information being offered for sale on the dark web.

Dyn (also known as the "Mirai" botnet attack) (USA): In October, a widespread distributed denial of service (DDoS) attack on this domain name service (an essential part in guiding internet browsers to the intended domain, which typically serves a website) saw their servers taken offline a number of times. This attack was broadly staged by making use of the plethora of internet-facing devices (through the "Internet of Things" connecting smart devices such as cameras, thermostats, etc.) that were infected with the Dyn malware. This outage affected access to many popular sites such as Twitter, Netflix, Airbnb and The New York Times.

Tesco Bank (UK): In November, the retail banking subsidiary of this UK supermarket fell victim to a hack which occurred most probably through its online banking system. Around 40 000 accounts were affected, almost half of which saw hundreds or thousands of pounds in unauthorised transactions. The company repaid £ 2.5 million of effective losses to 9 000 of its customers. Security experts and regulators have described this heist as an unprecedented attack on the UK's banking sector.

(1) References:
- Bank of Bangladesh: https://www.ft.com/content/39ec1e84-ec45-11e5-bb79-2303682345c8.
- Democratic National Committee: https://www.ft.com/content/d8ddee0e-5168-11e6-9664-e0bdc13c3bef.
- Yahoo !: https://www.ft.com/content/0ebde3b4-80fb-11e6-8e50-8ec15fb462f4.
- Dyn/Mirai: https://www.ft.com/content/d9b8445a-98d0-11e6-8f9b-70e3cabccfae.
- Tesco Bank: https://www.ft.com/content/a0300790-a4ba-11e6-8b69-02899e8bd9d1.

Any potential target that wishes to defend itself comprehensively against cyber attacks must evidently cover all aspects of its information flow, where both *confidentiality* and *availability* are essential to maintain. However, while compromising the *integrity* of its information is often more complex than any impact on *confidentiality or availability* (as access privileges generally need to be escalated further), safeguarding this aspect is often new terrain, where an institution is faced with a plethora of novel and often creative attack patterns. This is partly due to the increased sophistication of cyber criminals, taking their time to become accustomed to the procedures and technical intricacies of the institution under attack, allowing them eventually to tailor their approach into a highly effective attack. This requires targets to be equally flexible and nimble in their cyber stance, in order to improve the chances of being hardened against this.

Furthermore, a holistic stance towards their protection is advised, including not only the organisation itself, but also the counterparties with which it interacts, and the community as a whole. In this tightly interconnected financial ecosystem, most if not all transactions (and/or relating information) go through multiple parties before reaching their destination, many of them being FMIs, but also infrastructure operators and payment service providers. For criminals, this offers a multitude of attack vectors to focus on during the lifetime of a business interaction, and from the point of view of a transaction, one can only be hardened against fraudulent attempts if all steps in the chain are adequately secure.

In the following sections three best practices are discussed, as well as the related policy measures and regulatory initiatives. Section 1 elaborates on penetration testing and red team exercises as techniques to acquire reasonable assurance on the effectiveness of an organisation's protection, detection, response and recovery capacities. Section 2 discusses the need to share information to cooperate with partners in the ecosystem. Section 3 deals with endpoint security for FMIs. The article concludes with an overview of international coordination in the context of cyber security.

1. Penetration testing

Penetration tests are performed to identify vulnerabilities and attack vectors that can be used to exploit business systems successfully. This practice can vary widely in depth and with it, the resulting findings it can uncover. In its simplest form, automated tests are run on parts of the system to uncover some of the more conspicuous security issues. A more robust and encompassing form of assurance can be found in red team exercises. These put a team of outside specialists (the "red team") to assess the all-round security of an organisation by attempting to compromise it, often applying tactics and techniques closely resembling those of a criminal staging a similar attempt (that then has less noble goals). If well executed, the latter type of exercise provides a more realistic picture of an organisation's security stance than exercises that are automated, prepared, and/or announced. Furthermore, the red team may trigger active controls and responses during its campaign, not just limiting the assessment to the effectiveness of protection measures, but also putting an enterprise's detection, response, and recovery capabilities to the test. Of course, the assurance obtained is doubly effective if these exercises are not taken as a snapshot in isolation, but are well-prepared and well-followed-up, long before and after the actual tests take place. This requires sufficient maturity of the information security governance within the organisation, but equally of the security specialists that are performing the tests and guiding the organisation through preparation and debriefing.

Many regulators are working with the industry to encourage adoption of this practice, and to assist the organisations within their jurisdictions with its implementation and execution. One prime example of this is the Bank of England's CBEST[(1)] initiative. The initiative offers a testing framework designed to give major financial institutions and their regulators better insight into their vulnerability to cyber attacks, and the effectiveness of the measures in place. The main innovation of this framework has been in defining a scope much closer to what is essentially at stake, thus reflecting the ongoing strategic battle between cyber attackers and financial institutions. This tends to shift focus away from attempting a definite protection against attacks, a contingency which is, for all practical purposes, impossible to accomplish and might actually lead to complacency and a false sense of security. Rather, the framework seeks to improve an institution's resilience encompassing prevention, detection, response, and recovery as essential capabilities to cope with the full lifecycle of a cyber attack (i.e. including its potential materialisation and aftermath). In this vein, the red team exercises are an essential component put forward by CBEST. Furthermore, the framework ensures that the security experts are competent to perform these tests by subjecting them to accreditation by the Council for Registered Ethical Security Testers (CREST)[(2)].

2. Information sharing

A further cornerstone of the CBEST initiative is the promotion of broad information-sharing in the financial services sector. As mentioned earlier, this is a necessary venture that encourages an institution to recognise the ecosystem it is a

(1) CBEST is an intelligence-led vulnerability testing framework that has been devised by the UK financial authorities (the Bank of England and the Financial Conduct Authority) in conjunction with CREST (the Council for Registered Ethical Security Testers). For more information, see http://www.bankofengland.co.uk/financialstability/fsc/Pages/cbest.aspx.
(2) http://www.crest-approved.org/.

part of, and with which it shares the general challenges of cyber security. Two broad purposes this information can serve are being distinguished, as characterised by the urgency behind its content. Firstly, there is the information coming from a (potential) breach. Through their business relationships, an institution's direct counterparts may be directly exposed to the effects of such a breach. This requires an institution not only to be prepared for fraudulent incoming traffic, but also – as a sender – to clearly and promptly inform its correspondents of any compromises on its side should they occur. Whereas details of such events will also be reported to local law enforcement agencies and relevant regulators, this does not rule out the need to further reach out to the community by informing the market infrastructures that interconnect it. Furthermore, relevant Information Sharing and Analysis Centres (ISACs) and Malware Information Sharing Platforms (MISPs) offer an opportunity to contribute to common knowledge and insight across the ecosystem, much like on the attacking side: criminals often pool their tools and resources to raise the sophistication of their attacks. Participation in ISACs is therefore a practice that is a crucial element of an industry's resilience, and one which is strongly encouraged.

These ISACs/MISPs also play a fundamental role in divulging this information for its second purpose, one which satisfies more of a long-term, preventive necessity. While indeed the knowledge discussed before served in assisting the immediate reaction to current breaches, its value does not disappear afterwards. These early warnings can still be further analysed and assembled for the community to strengthen its preparations, a function often fulfilled by ISACs. This can result in a positive feedback loop to the benefit of the whole ecosystem: all players in the community contribute information to ISACs, which can then provide informed cyber intelligence such as indicators of compromise and best practices back to the community. This allows all parties access to expertise, allowing them with time to raise the sophistication of their resilience to threats. In this interaction, authorities are certainly not relegated to the sidelines: as well as being a part of this ecosystem, often with their own information and know-how to contribute, this interaction between players can only be optimally constructive given a fitting framework for information exchange. This requires a coordinated and balanced approach between different fields of regulation, such as financial stability, conduct, and privacy[1]. There can also be tremendous value in interacting with other sectors such as the energy and telecoms sector, as financial institutions are certainly not alone in their challenge against these threats.

3. Endpoint security for FMIs

FMIs play a central and systemic role in the efficient functioning of the global financial system. They often aggregate transactions both in volume and in value, and could therefore make them an interesting target for cyber criminals. Strengthening FMIs against any disruption that fraud or criminal attacks on their services can cause is therefore of the utmost importance.

Besides this direct aspect of securing these infrastructures, there is another important role for FMIs: it is through them that the best part of the financial system is interconnected, and this offers an almost natural channel through which fraud can be directed. This interconnectivity lays bare the exposure of any participant in the financial system not only to the security of the FMIs through which it connects, but also to the counterparties that the participant is connected with.

Core to this is a need for any interconnected system to be hardened as a whole, which is a more stringent condition than a sufficient hardening (however advanced) of the central nodes. In essence, any party in a transaction needs sufficient trust that the information encoding a transaction has been kept secure at every step along its way towards its destination: end-to-end security of transactions.

Recent developments such as the Bank of Bangladesh incident have exposed the limits of individual authorities to fully protect these end-to-end flows of the institutions in their jurisdiction. While the regulatory community is moving quickly to coordinate efforts, the centrality of FMIs extends to a responsibility that it has towards its community. That is to say, on top of the immediate responsibility for securing its own infrastructure, and preventing it from being directly compromised, it should also require a level of hardening to be taken up by the FMIs' participants. This unique central position that an FMI has between its participants is what allows it to hold them to high standards, in joint accountability towards keeping the FMI itself secure, and ultimately the entire counterparty community. Since essentially all parties are

(1) See also Caron, F. (2016), *Cyber risk response strategies for financial market infrastructures: towards active cyber defence*, NBB Financial Stability Report, 171-185 (https://www.nbb.be/doc/ts/publications/fsr/fsr_2016.pdf). and Caron, F. (2015), *Cyber risk management in financial market infrastructures: elements for a holistic and risk-based approach to cyber security*, NBB Financial Stability Report, 169-184 (https://www.nbb.be/doc/ts/publications/fsr/fsr_2015.pdf).

at risk of cyber attacks through these channels, this mission to harden the information flows end-to-end can only benefit the community at large.

Currently, this responsibility of FMIs and their participants is highly implicit. The final section will cover some recent efforts that are being undertaken to determine and harmonise the different roles. A key question here is on which party it will fall to set the requirements, enforce them, provide assurance and verify compliance, since these are still necessary elements for maintaining a level of trust that is essential in obtaining financial stability.

4. International coordination

As cyber criminals operate across and from remote jurisdictions, complicating criminal prosecution, and as financial markets themselves are more and more interconnected across borders, an open dialogue and cooperation between all regulatory authorities is necessary to avoid an asymmetry in their respective speed of action. In this cooperation, the ultimate goal is the advancement of the entire ecosystem's resilience in this continuing battle. In this respect, significant efforts have already been made as the regulatory community is actively promoting further hardening of defences.

As a notable example of this, in June 2016 the BIS Committee on Payments and Market Infrastructures (CPMI) and the International Organisation of Securities Commissions (IOSCO) published their "Guidance on cyber resilience for financial market infrastructures". Inspired by the industry's ongoing endeavours in this area, this guidance aims to offer a coordinated approach, and to foster international consistency in these efforts. This document offers comprehensive guidance in pre-empting cyber attacks, responding rapidly and effectively to them, and achieving faster and safer recovery objectives if they succeed. Alongside the elements of identification, protection, detection, response and recovery, a key concept in this guidance is also the governance aspect, where board and senior management attention is critical to a successful cyber resilience strategy. This guidance is to be applied to the FMIs under the Bank's oversight.

Building further on this guidance on cyber resilience, and sparked by the heightened impact on FMIs and wholesale payments, a new initiative has emerged within the CPMI. It has recently established a task force looking into the end-to-end security of wholesale payments that involve banks, FMIs and other financial institutions (i.e. cyber security in endpoints of payment system networks), thus recognising the increasing attention of cyber criminals towards the high-value transaction chain.

Enabling technologies in financial market infrastructures and payment services innovation : An overseers' perspective on opportunities, risks and policy

Filip Caron

Nimble technology firms are eating the lunch of traditional financial institutions, a recurrent statement in the financial press, literature and at conferences. But while FinTech is often considered as a collective noun for (start-up) disrupters in the financial industry, the concept was originally coined to describe the intersection between finance and technology.

Belgium-based financial market infrastructures (FMIs), custodians, payment service providers (PSPs), as well as critical service providers (CSPs) have a long tradition of technology-driven innovation in their business processes. At the same time, disruptors and digital giants have demonstrated significant interest in revisiting traditional business processes. This trend is partially driven by the rapid development of enabling technologies, the need for operational excellence and expectations for customer intimacy.

Two approaches to business process innovations are generally being distinguished : improving the efficiency and/or effectiveness of existing business processes and extensive business process redesigns. Increasing the speed, transparency and tracking of transactions without changing the processing flow are examples of the former (observed in e.g. SWIFT's Global Payments Innovation Initiative, see section 4 on SWIFT). Disintermediation like in Bitcoin, on the other hand, is an example of a significant business process redesign as it renders certain functions obsolete.

This article points up technology-induced paradigm shifts with a potential impact on FMIs and payment services in the longer run (section 1). Focus is on the future stable section of the hype curve, which follows the peak of inflated expectations and the trough of disillusionment[(1)]. The article discusses the most important risk drivers (section 2) in the technology (r)evolution and concludes with the overseers' main policy principles (section 3).

1. The potential of enabling technologies

Technological innovation and finance have long since gone hand in hand. The next wave of financial technology has been triggered by the abundance of recent technological advances such as the ubiquity of the internet, the availability of high-speed computing, cryptographic progress and innovations in data analysis.

(1) The Gartner Hype Curve or Cycle represents the maturity and adoption of new technologies in five key phases. After the initial stages of new technologies (technology trigger, peak of inflated expectations, trough of disillusionment), the technology's life cycle enters a phase where more deliverables benefiting the industry start to crystallize (slope of enlightenment) and, finally, where mainstream adoption or implementation starts to take off (plateau of productivity). Focus of this article is put on the last phase of the Gartner Hype Cycle.

Ingenious combinations of technologies could lock in interesting benefits and process improvements for the financial industry. For example, Bitcoin combined a variety of technologies such as digital signatures and peer-to-peer practices to develop an electronic payment system based on cryptographic proof instead of trust.

While these ingenious combinations are commonly referred to as enabling technologies (e.g. distributed ledger technology, see below), they are in their early stages of development. A series of important design decisions still need to be made and unsolved problems tackled before the full potential of these technology combinations can be realised. Consortia of various stakeholders are currently working on standard proposals.

This section describes three categories of promising enabling technologies: (1) distributed ledgers, (2) application programming interfaces, as well as (3) big data and artificial intelligence. For each enabling technology, the prospective benefits and potential impact on FMIs and financial services will be discussed.

DISTRIBUTED LEDGER TECHNOLOGY

Finance professionals, venture capitalists and regulators have been struck by the potential of distributed ledger technology (DLT), which focuses on providing access to trustable and complete data in networks without centralised data storage. A distributed ledger can be defined as a consensus on data replicated, shared and synchronised over a network. Replications of the data can be geographically spread and dispersed over multiple entities.

These ledgers could record ownership of a broad variety of assets. Typically, a distinction is made between digital assets that originate on the ledger (i.e. native assets such as virtual coins) and digital representations of physical assets (i.e. tokenised assets like unallocated gold). Hence, a multitude of potential use cases has been put forward; including global (wholesale) payments and securities, collateral management and corporate actions.

DLT has the capacity to open up considerable opportunities for efficiency gains. Primarily, DLT has the potential to disintermediate the trusted middlemen with a notary function. All entities participating in a DLT network can acquire real-time access to complete and accurate ledger data, which potentially reduces the frictions related to information sharing and reconciliation. Consequently, faster end-to-end processing of transactions becomes possible. As a network can comprise globally dispersed participants, these efficiency gains could also apply for cross-border transactions without a notary function as intermediary.

Additionally, DLT-based systems have the potential to strengthen data quality in the financial sector. Encryption technology can ensure the authenticity of the ledger data without recourse to central institutions and could guarantee the immutability of the data. Block chain is an oft-cited data organisation approach for DLT that focuses on cryptographically guaranteeing data immutability. Providing participants and trusted third parties (e.g. regulators) with access to full and immutable data, enables these parties to trace ownership and transaction history.

At the same time, DLT's near real-time data replication could assist financial institutions in reducing their operational and credit risk exposure. The pervasiveness of transaction data ensures strong data resilience, which is highly desirable in the event of a local system failure at an FMI or payment system provider. Additionally, this close-to-real-time data replication might ensure faster end-to-end processing.

The extent of these potential benefits might largely be determined by the proposed technology implementation, e.g. the scalability of the proposed implementation will likely impact the end-to-end processing speed. Currently, no convergence towards a generally accepted DLT implementation has been observed. As part of its technology assessment, the Bank has identified the governance arrangements, the data access restrictions, the synchronisation mechanisms and the underlying data structures as critical influencers for the quality of a DLT implementation. The Committee on Payments and Market Infrastructures (CPMI) recently published an assessment framework for DLT implementations[(1)].

(1) CPMI (2017), *Distributed ledger in payment, clearing and settlement – an analytical framework*, BIS (www.bis.org/cpmi/publ/d157.pdf).

In a scenario in which the core players were to adopt market-wide distributed ledgers, at least some peripheral players could be disintermediated[1]. This would be a significant process redesign. While this process could theoretically also render the settlement function of Central Securities Depositories (CSD) redundant, their disintermediation could be rather difficult from a legal point of view. Under the legal requirements of the Central Securities Depositories Regulation (CSDR)[2], securities subject to a transaction on a trading venue must be recorded in the books of a CSD prior to or at the latest on the intended settlement date. More generally, the potential efficiency gains of DLT can only materialise when its implementation matches fully within the existing legal environment. This might be achieved by adapting implementation, and where expedient from a public policy perspective, adapting the legal framework. While disintermediation of FMIs may result in less friction for end-to-end processing, it may also result in an abolition of certain risk reducing functions (e.g. netting), thereby reintroducing financial risks for participants.

APPLICATION PROGRAMMING INTERFACES (APIS)

Interoperability will be a key requirement for institutions wishing to benefit from a wealth of innovative solutions or aiming to connect to existing financial infrastructure, which is typically the case for respectively incumbents and start-ups. Structured interaction will be needed for information systems to invoke services from (e.g. creditworthiness assessments based on data from social media) and/or exchange data (e.g. account balances) between each other. The application programming interfaces (APIs) of an information system facilitate standardised access to the services and data offered by that system, and thereby enable automated interaction between systems.

APIs could unlock important opportunities for the creation of a new ecosystem. Contemporary financial institutions record a wealth of information on the behaviour of their customers that could be highly relevant for other organisations. By providing access to the data in a financial information system, for which consent and authorisation by individual customers will always be required, institutions could monetize the data. At the same time, APIs enable the integration of complementary services. Institutions can partner up with others to offer a more holistic and innovative product portfolio through their online platform. Similarly, they can take advantage of the API infrastructure of other institutions to broaden their distribution network.

Furthermore, FMIs, custodians, PSPs and CSPs could harness opportunities for reducing the regulatory cost and improving compliance assessments. The in-house development and maintenance of compliance tools (e.g. screening against sanction lists and anti-money-laundering services) can be notoriously complex and typically does not generate a competitive advantage. APIs enable institutions to invoke the services of externally developed and maintained compliance tools, sometimes referred to as regulatory technology or RegTech. Alternatively, institutions could use APIs to automatically collect sanction lists and/or collect know-your-customer details from a central depository.

Opening up the information systems to third-party service providers may result in an important increase of the cyber attack surface. Adequate mitigation measures will need to be put in place to ensure that access is restricted to trusted (authorised) third-party service providers. Furthermore, financial institutions will have to develop sound governance and risk management processes to ensure that the cyber security measures adopted by third-party service providers are appropriate. Any cyber event at a partner with a direct or indirect impact on the financial institution will likely have an impact on the institution's reputation.

Through the adoption of the Second Payment Services Directive (PSD2)[3], the European Commission has mandated account holding institutions to provide payment initiators[4] and account information services providers[5] access to the following services: the balance inquiry, credit transfer initiation and account identity verification services. Furthermore, the European Banking Authority (EBA) will develop a standardised specification for the APIs that need to be opened up

(1) Pinna, A. & Ruttenberg, W. (2016), *Distributed ledger technologies in securities post-trading*, ECB, Occasional Paper Series No 172 (https://www.ecb.europa.eu/pub/pdf/scpops/ecbop172.en.pdf).

(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 (http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0909&from=en).

(3) 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 (http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=EN).

(4) Third parties facilitating the use of online banking to initiate internet payments from the user account to the merchant account by creating a software "bridge" between these accounts, fill-in the information necessary for a transfer (amount of the transaction, account number, message) and inform the merchant once the transaction has been initiated.

(5) Third parties collecting and consolidating information on the different bank accounts of a consumer in a single place. These services will typically allow consumers to have a global view on their financial situation and to analyse their spending patterns, expenses, financial needs in a user-friendly manner.

under PSD2. In contrast, the technical specification for additional APIs may vary considerably. This would require financial institutions to adopt different interaction scenarios for different partners, which could be costly and therefore limit the overall interoperability in the industry.

APIs that allow organisations outside the financial industry to connect to PSPs will be crucial to facilitate automated payments in the Internet of Things context, e.g. cars automatically paying an insurance premium in a pay-as-you-go model, objects automatically paying for the energy they consume, refrigerators sending shopping lists along with payment credentials to an online grocery delivery store, or in pay-per-use object-sharing models.

FMIs and CSPs generally publish API specifications to enable direct connections between their clients' back office systems and their own information systems. These direct connections could lead to greater transaction processing efficiency, including enabling straight-through processing.

BIG DATA AND ARTIFICIAL INTELLIGENCE

The digital revolution has led to a huge increase in the scale of collection, processing and sharing of personal data. Hence, institutions seeking an information advantage have been collecting a wealth of data. Some of them start facing big data issues as it becomes computationally infeasible to process the datasets using traditional tools. These scalability issues are likely to arise in situations where the volume, velocity, variety and veracity of the data are considered high.

Artificial intelligence (AI) is being looked into to conduct data and behaviour analyses in a timely manner. AI is a set of advanced data analysis techniques that aim to mimick the cognitive functions of the human mind, e.g. deducing facts, reasoning, creative problem-solving for issues, representing knowledge, planning and social intelligence. Fintech start-ups are aiming at even further enriching the analyses by compiling data from different sources.

A variety of use cases for AI has been presented in FMIs and payment services, including obtaining detailed customer insight and fraud detection. Typical customer insight analyses relate to individualised and enhanced product offerings, upselling and churn prediction. Card scheme operators have successfully experimented with the identification of fraudulent transactions through behaviour analysis.

While data and behaviour analysis might result in clear competitive advantages, institutions must be cautious not to violate basic privacy principles. General legitimacy and purpose limitation principles dictate that data can only be processed for transparent predefined (or compatible) purposes. Big data projects, on the other hand, tend to focus on finding hidden relations between data variables and therefore could benefit from the reuse of data collected for other projects. While data anonymisation might allow for compliance with some basic privacy principles, there is often still the risk of re-identification based on data compilation.

2. Risks in a disrupted financial environment

The current wave of disruptive technologies and start-ups may pose significant opportunities for the financial industry. The right strategical decisions (e.g. ecosystem or utility provider visions) could well make the difference between the incumbents' survival and their demise. At the same time, innovations come with their own set of risks and challenges, including the usual set of operational (information and cyber), third-party, governance, legal and financial risks.

INFORMATION AND CYBER RISKS

Information and cyber security focus on reliable service delivery in a networked environment, i.e. guaranteeing the confidentiality, integrity and availability of information. In addition to the traditional cyber security threats, the particular characteristics of the FinTech ecosystem cause additional challenges.

FinTech solutions are often based on relatively immature internet-facing technologies, which may contain unforeseen vulnerabilities and other issues. Any failure has the potential to significantly undermine market confidence. Technology-testing scenarios must closely reflect real-life situations, and could be complemented with extensive penetration testing.

Furthermore, setting up effective (mature) authorisation and fraud detection mechanisms will be crucial in reliable service delivery.

Strong cyber security measures that foster detection, containment and recovery from cyber incidents will be required for all participants of the financial industry. AI is often cited as one of the most promising technologies in cyber threat detection, whereas active defence measures should enable to limit the impact of a materialising threat[1]. Extensive cyber security guidelines have been published in a CPMI-IOSCO joint guidance report[2] and an overview of strategic, tactical and operational controls has been discussed in a previous publication of the Bank[3].

THIRD-PARTY RISKS

Financial ecosystem strategies are based on the integration of services provided by a broad diversity of interconnected entities. Additionally, FinTech start-ups and increasingly incumbents are developing solutions based on third-party infrastructure- and software-as-a-service products as these products could result in significant cost reductions and scaling flexibility. As a result, an increasing exposure to interdependencies with third-party risk can be observed.

Adversaries might take advantage of vulnerabilities at a specific partner in the ecosystem, in order to gain access to the systems of other participants. Obtaining clear insight in the security policies and procedures, the downstream dependencies and the contingency measures of partners are commonly observed challenges in third-party relationships.

Establishing and enforcing common security baselines is considered a best practice for third party risk mitigation. Furthermore, the partners could consider to integrate their incident response processes and to put security assurance reporting models in place.

GOVERNANCE RISKS

Governance arrangements and exception handling are increasingly captured in programming code, with the Bitcoin block chain as an extreme example. Theoretically, codes would be extremely effective in enforcing these arrangements. In practice, there are significant limitations to the automated approach that require adequate attention : emerging technology risks and misuses of the system.

Establishing a governance structure could help contain the potential negative impact of emerging technology risks, e.g. to adapt the system design, security controls and or business rules. Research has indicated that vulnerabilities in software are all too common. Additionally, the effectiveness of security controls, e.g. the strength of a cryptographic scheme tends to fall off as computing capacity exponentially increases.

Adequate incident response processes should be specified in order to deal with undesired system behaviour that is not prohibited by the code. TheDAO[4] that aimed at codifying all governance rules and the decision making processes of an organisation, was confronted with a set of vulnerabilities that enabled the draining of significant amounts of funds without violating any of the encoded rules. While patches eliminating these vulnerabilities were publicly proposed but not approved by the community, approximately a third of TheDAO's funds were "maliciously" diverted to another entity.

The CPMI-IOSCO's Principles for Financial Market Infrastructures (PFMIs)[5] prescribe the need for formal governance arrangements that are charged with establishing risk management, internal control and incident management processes. Furthermore, these arrangements should provide clear and direct lines of responsibility and accountability. Effective governance bodies consist of members with integrity that have appropriate experience and skills (including expertise in both technology and finance).

(1) Caron, F. (2016), *Cyber risk response strategies for financial market infrastructures : towards active cyber defence*, NBB Financial Stability Report, 171-185. (https : //www.nbb.be/doc/ts/publications/fsr/fsr_2016.pdf).

(2) CPMI-IOSCO (2016), Guidance on cyber resilience for financial market infrastructures, BIS (http : //www.bis.org/cpmi/publ/d146.pdf).

(3) Caron, F. (2015), *Cyber risk management in financial market infrastructures : elements for a holistic and risk-based approach to cyber security*, NBB Financial Stability Report, 169-184. (https : //www.nbb.be/doc/ts/publications/fsr/fsr2015.pdf).

(4) A decentralised autonomous organisation (DAO) codifies governance and decision-making so that the organisation can be run by a computer program without human involvement. TheDAO is currently the most prominent example of this organisational type.

(5) CPMI-IOSCO (2012), *Principles for financial market infrastructures*, BIS (http : //www.bis.org/publ/cpss101a.pdf).

LEGAL RISKS

Two main drivers of legal risks have been identified: complexity related to determining the applicable regulation and conflicts between legal requirements and technology principles.

Start-ups may be operating in a less certain legal context, partly driven by the issue of determining the relevant jurisdiction and/or applicable regulation. FinTech solutions could, from a technical point of view, be provided globally through the internet. Additionally, determining the legal location of data can be cumbersome in a cloud environment or a DLT solution. A robust legal basis can be considered as critical to the overall soundness of new technology-enabled business models. A legal basis will facilitate the definition and enforcement of the rights and responsibilities of the relevant parties.

A second set of legal risks originates from divergent legal requirements and technology principles. For example, an FMI should be able to reverse a transaction in response to a mistake or a legal mandate (i.e. the correctability requirement), whereas a major principle in block chain and most DLT implementations is the immutability of the data. Furthermore, a mandatory fork, which basically results in discarding part of the chain and is the proposed reversing technique, might leave participants in the network exposed to legal claims. This was for example the case in the previously mentioned TheDAO incident[1].

FINANCIAL RISKS IN DLT

Significant uncertainty about settlement in DLT solutions remains, notably on the finality of a settlement in DLT solutions, as well as on the feasibility of implementing a genuine delivery-versus-payment (DvP) solution.

Certainty of settlement is achieved when a transaction is legally both final and irrevocable. However, in block-chain-based DLT designs, settlement is typically probabilistic, i.e. the longer a transaction is recorded in the ledger, the less likely the transaction will be reversed (or dropped) as the resources needed to change the chain of blocks significantly increases each time a block is added. Whether a probabilistic finality could comply with the requirements stipulated in the Settlement Finality Directive[2] remains untested.

A DvP securities settlement requires simultaneous finality of the transaction in both the security and cash ledger, which may imply synchronisation between DLT ledgers. Inter-ledger synchronisation is currently considered to be an important technical challenge with a legal impact.

3. Facilitating innovation, while guaranteeing stability

Regulators generally strive to facilitate innovation, security and competition in FMIs and payment services, while guaranteeing a level playing field for all market participants in terms of risk mitigation, prudential supervision and oversight.

RISK-BASED REGULATORY FRAMEWORK

Risk-based regulatory frameworks that focus on the provision of reliable and secure services enable regulators to be consistent in an industry that is liable to be (radically) reshaped by technological innovators.

The Bank rigorously follows up on technological innovations and assesses their (potential) impact on FMIs, custodians, PSPs and CSPs. This setting allows for innovative experiments, while enabling adequate regulatory response to risks and threats. As overseer and prudential supervisor of these systems and institutions, the Bank continues to focus on the importance of cyber and transaction security.

(1) https://blog.ethereum.org/2016/06/17/critical-update-re-dao-vulnerability/.

(2) Directive 98/26/EC of the European Parliament and of the Council of 19 May 1998 on settlement finality in payment and securities settlement systems, *OJ*. 11 June 1998, L.166, 45-50 (http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31998L0026&from=EN).

TECHNOLOGY-NEUTRAL

Regulators in general are committing themselves to the principle of tech neutrality in regulation. The actual type of technology will not be taken into account when defining the requirements for obtaining authorisations, risk mitigation and other responsibilities. These requirements are risk-based, and an implementation of a technology will be assessed on basis of these criteria.

Subjecting technology innovators to special regulatory treatment could result in a distorted playing field. The regulators should not overprotect incumbents and should enable the development of designs that are better aligned with their business models and their customers' preferences while reducing risks or maintaining low risks. An equal treatment for equals should be guaranteed.

Technology neutral regulation enables the regulators to adequately respond to technology evolutions and innovations.

DIVERSE INTERMEDIARY TYPES

Entrants targeting a specific niche of payments, clearing and settlement services might have a different risk profile (in terms of risk types) than generalist FMIs, custodians, PSPs or CSPs. In adapting to this changed reality, regulators could introduce new regulatory intermediary types.

For example, payment initiation and account information services are two new regulatory intermediary types specified in PSD2. A risk-based differentiation from the payment institute licence has been foreseen for these intermediary types, e.g. because they do not provide account-holding services, they are not subjected to the same capital requirements as traditional payments institutions.

SUPPORT THROUGHOUT THE AUTHORISATION PROCESS

The Belgian regulatory authorities, the Bank and FSMA, recently decided to set up a single point of contact (SPOC)[(1)] for developers of FinTech solutions and to share all relevant information on a web platform. The SPOC will provide assistance in identifying the type of licence that will be needed for the proposed solution, clarify the regulatory framework and assess the legal aspects of the business model, assist in compiling authorisation application files and follow up on the processing of authorisation requests.

INTERNATIONAL COORDINATION

The cross-border nature of technological innovation calls for international coordination amongst regulatory authorities, which should result in a consistent, standardised and transparent regulatory environment for the providers of FinTech solutions. Examples at European level include the PSD2 and the General Data Protection Regulation (GDPR)[(2)].

(1) https://www.nbb.be/en/fintech.

(2) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *OJ*. 4 May 2016, L.119, 1-88 (http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN).

Concentration risks in financial market infrastructures – the specific case of CCPs

Sven Siedlecki

Although the European post-trade landscape remains fragmented[1], from time to time there are mergers between post-trade financial market infrastructures (FMIs). There have been mergers between Central Securities Depositories (CSDs) (e.g. the Euroclear Group) and between central counterparties (CCPs) (e.g. the merger between EuroCCP (UK) and EMCF (NL) in 2013). While there may be benefits for shareholders and indeed for clearing members (CMs)[2] in the case of CCPs (see section 1 below), mergers between FMIs also involve risks for the wider financial system. Although some of these risks are applicable regardless of the type of FMIs that merge, the article will focus on CCPs (see section 2).

1. Drivers for mergers between CCPs

As with any merger between two companies, there are potential cost savings from economies of scale to be expected, which may benefit the shareholders of the company (if lower costs mean higher profits) and/or the clients (if lower costs mean lower prices).

In addition, a typical advantage of merging two CCPs lies in the extra netting and diversification effects of combining CMs' various (long and short[3]) positions. Via portfolio margining, a technique that calculates the CMs' margin requirements taking into account the correlations between their positions in various asset classes (see box 1), CMs can reduce their total margin requirements by combining their positions in different asset classes in one CCP. This means that CMs need to transfer fewer high-quality assets (the type of assets that CCPs typically require as margin) to the CCP to meet their margin requirements – something that is welcomed by the CMs – even more so after the obligation to clear standardised OTC derivatives in a CCP[4], which will require margin from the CMs to cover the risks on positions taken in these OTC derivatives. The clearing obligation may be a driver for mergers between CCPs, not only because it increases CMs' margin requirements (as standardised OTC derivatives are to be cleared in a CCP) and thus the need for margin-reducing techniques such as portfolio margining, but the clearing obligation also means that more products need to be cleared in a CCP and thereby enlarges the pool of assets of which trades can be netted through the interposition of CCPs which in turn leads to a greater potential netting effect.

(1) An overview of the post-trade landscape in Europe can be found in *Developments in the post-trade services environment in Europe*, NBB Financial Stability Review, 2014, 162-163 (https://www.nbb.be/doc/ts/publications/fsr/fsr2014.pdf).

(2) Members of a CCP that clear trades on their own behalf and/or on behalf of their clients.

(3) CMs' "long" positions refer to outstanding purchase obligations (e.g. in respect of a derivatives contract), while "short" positions refer to outstanding sell obligations.

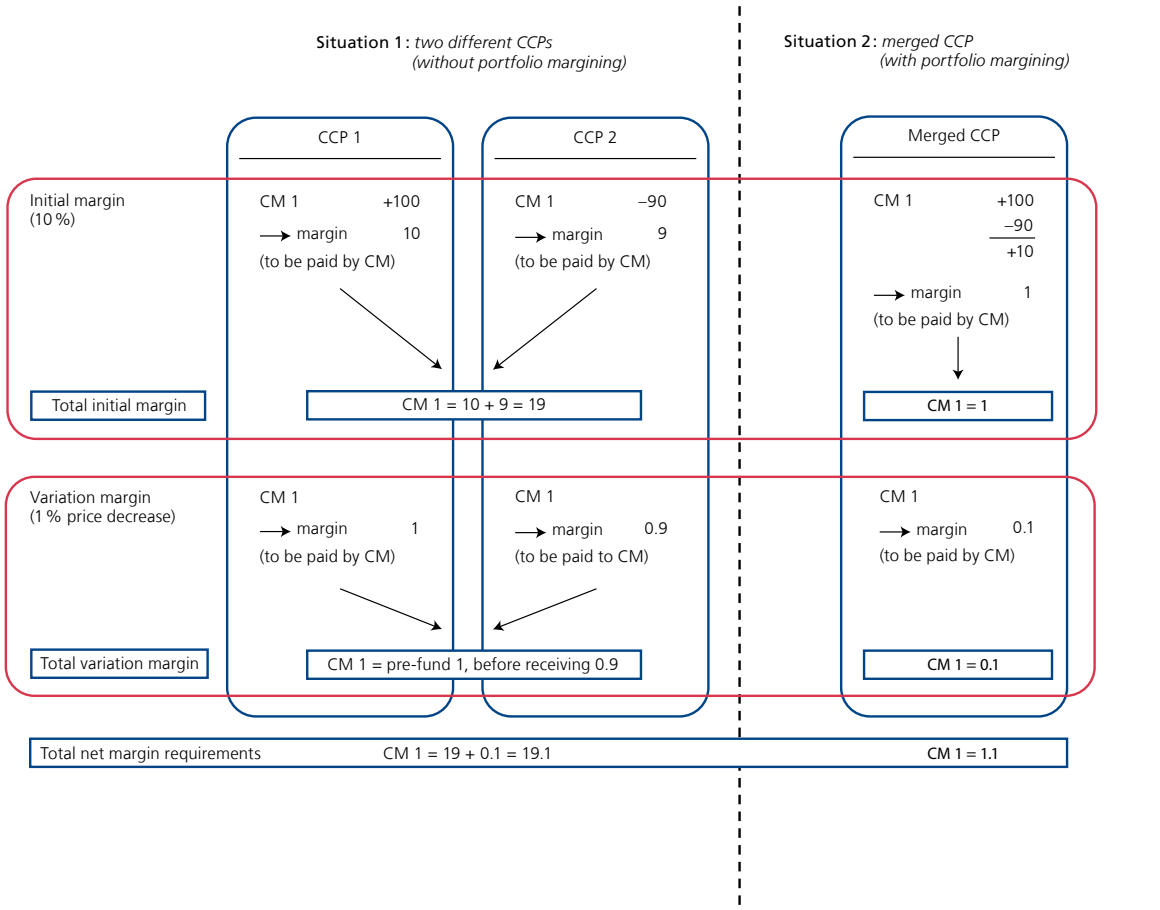
(4) E.g. under the European Markets Infrastructure Regulation (EMIR) in Europe and the Dodd-Frank Act in the US.

Box 1 – Portfolio margining

When a clearing member (CM) takes on a position in a product that is cleared in a CCP, the CCP steps in between the two counterparties (i.e. the CCP becomes the buyer of every seller, and the seller of every buyer). A CCP requires a pre-set amount of collateral – called initial margin – to be posted by each CM in a transaction to cover the CCP's potential future exposure on the CM's position over the liquidation period (i.e. period needed to hedge or close a position in normal markets). In case of a default, the defaulting CM's initial margin can be used or liquidated to cover any losses or obligations that are incurred. EMIR requires that the length of the liquidation period is set in accordance with the contract type (standard minimum length of one or five days respectively for on-exchange and OTC contracts). The size of the initial margin depends on the volatility of the contract (i.e. observed price movements over the last 10 years). The initial margin should cover 99 % (99.5 % for OTC derivatives) of the price movements over the liquidation period (in the stylised example below, 10 % initial margin is required by each CCP).

The CCP calculates daily (or more frequently) the gains and losses on each CM's portfolio (mark-to-market value) and transfers cash from the CM that loses to the CM that gains, i.e. the payment of the variation margin. This

STYLISED EXAMPLE OF PORTFOLIO MARGINING



Source: NBB.

limits the build-up of exposures arising from changes in market prices over the life of the contract. Such exchange of variation margin occurs every day, but when the CM defaults and does not make any variation margin contribution, the CCP needs to be covered against adverse price fluctuations for the period during which the CM's positions are closed out.

Situation 1 on the left-hand side of the graph is a situation with two CCPs where the margin requirements for the CM are calculated independently. CM 1 has positions in products that are economically identical (perfect correlation of 1, in order to avoid complexities of correlations between different products that may break down in crisis situations and to focus on the effects of a merger between CCPs in the stylised example). In CCP 1, the CM has an outstanding purchase obligation ("long position") of 100 and in CCP 2 it has an outstanding sell obligation ("short position") of 90. As each CCP calculates its own risk and margin requirements independently, the CM needs to post 10 (10 % to cover the long 100) and 9 (10 % to cover the short 90), or a total of 19 as initial margin to the two CCPs. Furthermore, if the price falls by 1 %, the CM will need to pay a variation margin of 1 (1 % of +100) to CCP 1 and receives 0.9 (1 % of –90) from CCP 2. As the deadline to pay the variation margin (pay-in) is typically before the CCP pays out the variation margin to the CM (pay-out), the CM will need to pre-fund 1 to be paid to CCP 1 until it receives 0.9 from CCP 2.

Situation 2 shows the impact of portfolio margining when the two CCPs merge. CM 1's portfolio now consists of 100 long and 90 short in products that are perfectly correlated, reducing the net risk to the merged CCP to 10, which only requires an initial margin of 1 (10 % to cover the net position 10). In addition, CM 1 only has to pay variation margin for the net position of +10, meaning it will only have to pay 0.1 (1 % of +10) by the pay-in deadline.

As shown in the graph below, by merging CCPs, CMs can benefit from portfolio margining and reduced total margin requirements (1.1 versus 19.1 for respectively with and without portfolio margining). In a real-world situation, the margin reduction may not be that spectacular (as in practice, CMs will not concentrate, for perfectly correlated products, their long positions in one CCP and their short ones in another CCP), but CMs can still benefit from reduced margin requirements as a diversified portfolio is less volatile than individual products.

2. Risks from concentration of CCPs

As described in section 1, the pooling of asset classes in a single CCP and the related benefits of the increased netting effect are incentives for mergers between CCPs and may lead to natural oligopolies or monopolies.

While a concentration of CCPs (via a legal merger or intra-group arrangements) may bring benefits to its shareholders – and even to its CMs – such concentration also increases financial stability risks.

CONTAGION RISK BY CO-MINGLING OF EXPOSURES ON DIFFERENT MARKETS

By merging CCPs that clear different financial products, CMs can benefit from portfolio margining and lower total margin requirements. On the other hand, such concentration may cause contagion as the merged CCP could serve as a channel through which stress in one market contaminates other markets.

OPERATIONAL AND FINANCIAL CONCENTRATION RISKS

An operational problem (e.g. a cyber attack – see article Cyber security in financial market infrastructures) at a merged CCP, or CCPs that belong to the same corporate group and that share a common IT infrastructure, will have a wider impact. Similarly, a concentrated CCP that defaults can spread risks to various parts of the financial system. In addition, effective recovery and resolution of a large CCP that is active in different markets (in terms of geography or asset classes) may be more complicated, including finding an alternative CCP in such a concentrated market. Although losses caused

by the default of a CM are mutualised among CMs (via the CCP's default fund[1], the haircutting of CMs' variation margins gains or writing down initial margin provided by non-defaulting CMs), the capital of the CCP itself is also at risk and some CCPs include additional financial support (such as a parental guarantee) in their rule book[2]. The actual ability of the CCP's parent company to provide this support could be hampered if this parent company holds multiple/large CCPs.

SYSTEMIC RISK BY INCREASED LEVERAGE IN THE FINANCIAL SYSTEM

Even if CCPs that clear the same market merge, this could lead to an increase in systemic risk. By pooling long and short positions in one CCP, the CMs can benefit from a netting effect and thus lower margin requirements. This reduction of margin requirements frees up high-quality assets for the CMs, which could then be used as margin to cover additional transactions, enabling them to take on more risk. While the merged CCP is still sufficiently covered in terms of market risk even though it requires less margin for a portfolio of netted long and short positions, the whole financial system may become more risky as traders have more leverage capacity – and can thus take more risks – with the same amount of high quality assets. In addition, the CCP itself may become more risky in terms of operational and liquidity risk, as closing out a position of 100 (long) and 90 (short) in different but nettable products, as in the example of box 1, may not be the same as dealing with an original position of just 10.

3. Potential systemic implications

Unlike the European Commission's analyses of mergers and acquisitions from a competition point of view, there is currently no authority in the EU responsible for ex ante authorising a merger of CCPs on the basis of systemic risk implications. Legislation like EMIR is aimed at ensuring that at individual CCP level, risks are adequately dealt with. However, current regulation does not adequately deal with general systemic risks to the financial system as a whole resulting from concentration among CCPs.

In the meantime, regulation could be enhanced in order to adequately take concentration risks into consideration. The default funds of CCPs that clear different markets are often split into different compartments to avoid problems on one market spilling over to CMs on other markets. In this way, the contagion effect of a multi-product CCP can be contained to some extent. When a CCP belongs to a group that encompasses other CCPs as well, a consolidated view is needed to assess the parent company's capacity to provide financial support if need be. Cross-border (groups of) CCPs call for close international cooperation between competent authorities, including in the area of recovery and resolution.

The potential increase in leverage in the financial system can be addressed by regulating the individual institutions where an increase in risk-taking would be undesirable. In addition, the conditions under which portfolio margining is allowed should be designed to avoid competition between CCPs on the basis of lower margin requirements. The European Securities and Markets Authority (ESMA) has already performed a peer review[3] of portfolio margining issues (e.g. there needs to be an economic rationale for offsetting positions, and there needs to be a significant and reliable correlation).

(1) CMs' contributions towards a CCP's mutualised loss sharing arrangement.

(2) Swerts, Q., Van Cauwenberge, S., *CCP resilience and recovery – Impact for the CCP users*, NBB Financial Stability Report 2016, 187-202 (https://www.nbb.be/doc/ts/publications/fsr/fsr_2016.pdf).

(3) ESMA (2016), *Peer Review under EMIR Art. 21 – Supervisory activities on CCPs' Margin and Collateral requirements* (https://www.esma.europa.eu/press-news/esma-news/esma-identifies-areas-improvement-in-eu-ccp-supervision).

List of abbreviations

ACH	Automated clearing house
AIFMD	Alternative Investment Fund Managers Directive
BCBS	Basel Committee on Banking Supervision
BNYM	Bank of New York Mellon
BRRD	Bank Recovery and Resolution Directive
CCP	Central counterparty
CDS	Credit default swap
CEC	Centre for Exchange and Clearing
CIK	Caisse Interprofessionnelle de Dépôts et de Virements de Titres (now Euroclear Belgium)
CLS	Continous Linked Settlement
CM	Clearing member
CMG	Crisis Management Group
CPMI	Committee on Payments and Market Infrastructures
CRD	Capital Requirements Directive
CREST	Council for Registered Ethical Security Testers
CRR	Capital Requirements Regulation
CSDR	CSD Regulation
CSD	Central Securities Depository
CSP	Critical Service Provider
DDoS	Distributed denial of service
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
EFTA	European Free Trade Association
ELMIs	Electronic money institutions
EMD	Electronic Money Directive
EMEA	Europe, Middle East and Africa
EMIR	European Market Infrastructure Regulation
ESA	Euroclear SA/NV
ESCB	European System of Central Banks

ESES	Euroclear Settlement of Euronext-zone Securities
ESMA	European Securities and Markets Authority
ETF	Exchange-traded fund
EU	European Union
FCA	Financial Conduct Authority
FMI	Financial market infrastructure
FRA	Forward rate agreement
FSB	Financial Stability Board
FSMA	Financial Services and Markets Authority
FX	Foreign exchange
G-SiFI	Global systemically important financial institution
ICMA	International Capital Markets Association
ICSD	International central securities depository
IFR	Regulation on interchange fees for card-based payment transactions
IOSCO	International Organisation of Securities Commissions
IRS	Interest rate swap
ISAC	Information Sharing and Analysis Centre
LEI	Legal entity identifier
LSE	London Stock Exchange
LSI	Less significant institution
MCE	MasterCard Europe
MISP	Malware information sharing platforms
MoU	Memorandum of Understanding
MTU	Margin transit utility
NBU	National Bank of Ukraine
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
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
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
TFPS	Task Force on Payment Services
UCITS	Undertakings for the collective investment of transferable securities
VM	Variation margin

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

Marcia De Wachter

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 – Fax +32 2 221 31 90
johan.pissens@nbb.be

Cover and layout: NBB AG – Prepress & Image

Published in June 2017