Financial Market Infrastructures and Payment Services Report

2019

National Bank OF BELGIUM
Eurosystem

Financial Market Infrastructures and Payment Services Report

2019

National Bank OF BELGIUM
Eurosystem

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

N. Boeckx, K. Bollen, F. Caron, D. De Beuckeleer, P. Gourdin, J. Jans, I. Meau, L. Ohn, F. Saffer, C. Stas, R. Temmerman, M. Van Acoleyen, S. Van Cauwenberge, I. Vansieleghem, J. Vermeulen

Contents

Executive summary

2018 may be marked as a tipping point for the retail payments area in Belgium and in Europe with the implementation of the Payment Services Directive (PSD2). The changes it is inducing in business models, as well as the emergence of instant payments, will further shape the sector in 2019 and the years ahead. Another major event impacting every component of the financial markets, not least in Belgium, is Brexit. Against this background of structural and strategic challenges, cyber resilience continues to be top of the agenda for risk managers and regulators.

PSD2

On the legal front, national and European authorities have introduced major regulatory changes in order to further shape Europe as a dynamic, innovative and secure retail payments market. The PSD2 has been transposed into national law in most of the EEA countries. Services recently explored by FinTech companies such as initiation of payments and account information delivery – without holding the payment service user's payment account – have been singled out and defined as regular payment services. These new services aim to create an open banking infrastructure and may trigger disruptive movements in the payment services area. They constitute major challenges for incumbent payment service providers, mainly the banks, although the latter are also preparing to incorporate new services and adapt their product range.

In Belgium, the Bank and the Federal Public Service (FPS) Economy have both taken on responsibility for implementing PSD2, that is, the Bank for the prudential supervisory regime for payment services, and FPS Economy for the new regulatory issues on consumer protection measures and rights and obligations for payment service providers. All existing licence-holding institutions have had to demonstrate compliance with the new requirements, including those on security of payments. Most institutions have been re-authorised by the Bank, but some had to cease their activities.

Instant payments

Dynamic and innovative retail payment services are being developed and are affecting the payment systems landscape. In Belgium, as in several other European countries, new payment schemes and far-reaching changes to payment systems are emerging. In 2018, the main focus of the Belgian domestic retail payments system (CEC) was to prepare for the implementation of instant payments launched in March 2019. The impact of such a change cannot be under-estimated as it brings ubiquitous real-time payments to the public 24/7/365.

Brexit

Payment flows in the EEA will to a large extent be redrawn as a result of Brexit. The clearing of the Belgian repo market for government debt has been shifted end of 2018 from the London clearing house LCH Ltd to Paris-based LCH SA. From a financial stability point of view, it means that this activity is now being processed by an institution established in the eurozone with access to central bank services in euro. In the sector of payment service providers, several UK payment institutions have approached the Bank and applied for a licence as a

Belgian payment institution to be in a position to continue – after Brexit – providing services in the EEA through a new licensed Belgian entity.

Cyber resilience

Apart from physical security, digital security remains key for Financial Market Infrastructures (FMIs) and providers of payment services. International standard-setting on cyber resilience has further developed and the Bank is now using available international frameworks extensively for all infrastructures and payment service providers under its supervision and oversight regime. For example, in May 2018, the Committee on Payments and Market Infrastructures (CPMI) presented a strategy to encourage and help focus industry efforts towards reducing the risk of wholesale payments fraud related to compromised customer IT infrastructures (Strategy for reducing the risk of wholesale payments fraud related to endpoint security). The Governors of the BIS Global Economy Meeting (GEM) expressed their support for and commitment to operationalising the strategy within their institutions and jurisdictions. Also, the December 2018 ECB *Cyber Resilience Oversight Expectations for FMIs*, or CROE, gives further guidance on cyber resilience requirements for FMIs published by the CPMI and the International Organisation of Securities Commissions (IOSCO) in June 2016.

Another tool that will be used by the Bank is the ECB European Framework for Threat Intelligence-based Ethical Red Teaming (TIBER-EU), which is the first European-wide framework for controlled and bespoke tests against cyberattacks in the financial market. It will facilitate a harmonised European approach towards intelligence-led tests which mimic the tactics, techniques and procedures of real hackers who can be a genuine threat. In 2018, the Bank set up such a framework in Belgium (TIBER-BE) that will be rolled out in the course of 2019.

Due to their interconnectivity, should an FMI fall victim to a successful cyberattack, it could lead to systemic consequences on the global financial markets, possibly even with a loss of confidence in the financial system. The cyber resilience of FMIs is therefore essential for the stability of the financial system. Cooperation and coordination are key both at national and international level, between regulators and between FMIs. In addition, joint forums of regulators and FMIs have been established, such as the Financial Sector Cyber Council (FSCC) in Belgium and the Euro Cyber Resilience Board for pan-European FMIs. The challenge of overcoming threats of large-scale cyberattacks is huge, but all financial sector stakeholders (FMIs, regulators/overseers, payments institutions, retail banks, etc.) are working together to improve contingency planning and set up a global response to this systemic risk.

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

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

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

The systems and institutions covered in this Report can be ranked in three categories according to the type of service provided : (i) securities clearing, settlement and custody, (ii) payments and (iii) other market infrastructures and critical service providers to the financial infrastructure. Through their activities or services provided to the financial industry, these systems and institutions are the critical nodes in the functioning of financial markets and payment services as well as the real economy. If designed safely and managed properly, they are instrumental in reducing systemic risks and contagion in the event of financial crisis. At the same time, they are interlinked with other FMIs, financial intermediaries and other actors such as merchants or retail customers. These interdependencies are briefly presented and illustrated in chart 1. Box 1 shows how these systems and institutions providing payment, clearing, settlement, custody and other services have performed between 2008 and 2018 in terms of transaction volumes and values.

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

FMIs and financial institutions that provide securities clearing, settlement and custody services are considered part of the post-trade securities landscape. The clearing of a trade via a central counterparty (CCP) generally means that the CCP becomes the buyer counterparty for the seller and the seller counterparty for the buyer. Both original counterparties to the trade then have a claim on the CCP. The direct participant of a CCP – usually

a bank or an investment firm – is called a clearing member. A clearing member may clear not only its own trades via the CCP, but also those of its clients. Whereas there are no CCPs established in Belgium, CCPs in other countries can be systemically important due to their clearing activities for the Belgian securities market.

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

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

Payments

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

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

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

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.

a major role in providing money transfer/remittance services (fund transfers) allowing retail customers to transfer cash from Belgium to a third party in different locations around the world and vice versa.

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

Other market infrastructures and critical service providers

TARGET2-Securities (T2S) is the common settlement platform for European CSDs. Although SWIFT is neither a payment system nor a settlement system, a large number of systemically important systems depend on it for their daily financial messaging. It is therefore considered as a critical service provider.

BOX 1

Growing importance of payment and settlement systems, FMIs and other service providers in the payment area

The years between 2008-2018 were marked by the break-out of the financial and sovereign crisis, by the implementation of monetary policy measures to soften the impact of those crises, as well as by new regulation aiming to avoid their re-occurrence in the future (e.g. EMIR clearing obligation). In parallel, this period also saw the advanced digitalisation of payments processing.

The underlying parameters that could explain the evolution in FMIs' and service providers' business activities can be diverse (e.g. market volatility in wholesale markets, digitalisation of retail payments). The chart below shows for a selection of systems and institutions the business growth rates between 2008 and 2018 (with 2008 as the reference year). Some of them have expanded their activity considerably. In terms of transaction volumes, this is notably the case for Euroclear Bank (+154 %) and SWIFT (+104 %)[1]. In value terms, highest growth rates are recorded for Euroclear Belgium (+188 %)[2] and Euroclear Bank (+86 %). Others have also grown but less significantly (e.g. retail payment system CEC) or were subject to more volatility (e.g. NBB-SSS due to impact sovereign crisis).

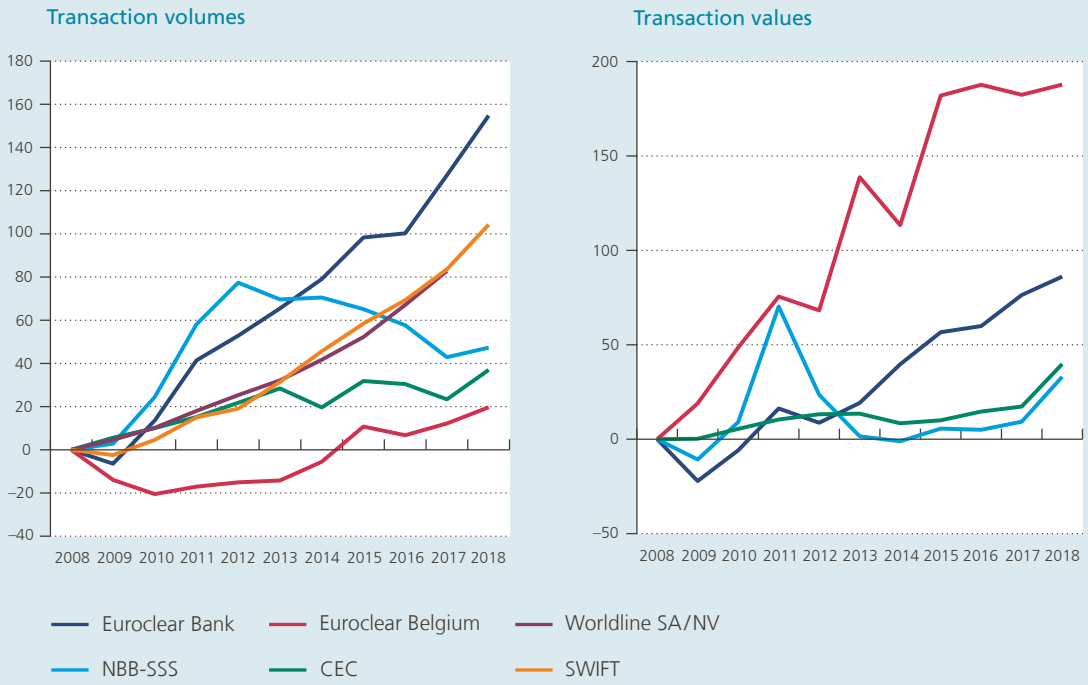
In general, the systemic importance of these systems and institutions continues to grow. An unexpected disruption of those systems and institutions could have a significant impact widespread across different types of stakeholders (including the public in general). Should payments between market participants fail, one of the counterparties could for example be faced with acute liquidity risks. Operational incidents can be *fast burning* disturbing businesses and society at large provoking economical damage to individuals (retail perspective) or to financial markets and monetary policy (wholesale perspective). *Slow burning* scenarios (cyber, data integrity) could impact confidence in the financial system. Operational resilience of FMIs and

1 Worldline SA/NV data for 2018 not available.
2 Euroclear Belgium settles mainly equities that are expressed in terms of market value.

other service providers in the payment area is therefore a top priority for regulators, both with respect to day-to-day operational risk management (e.g. capacity management, system change plans) and contingency situations (e.g. business continuity plans, disaster recovery plans), including in case of cyberattacks.

Evolution of transactions processed by selected FMIs and service providers

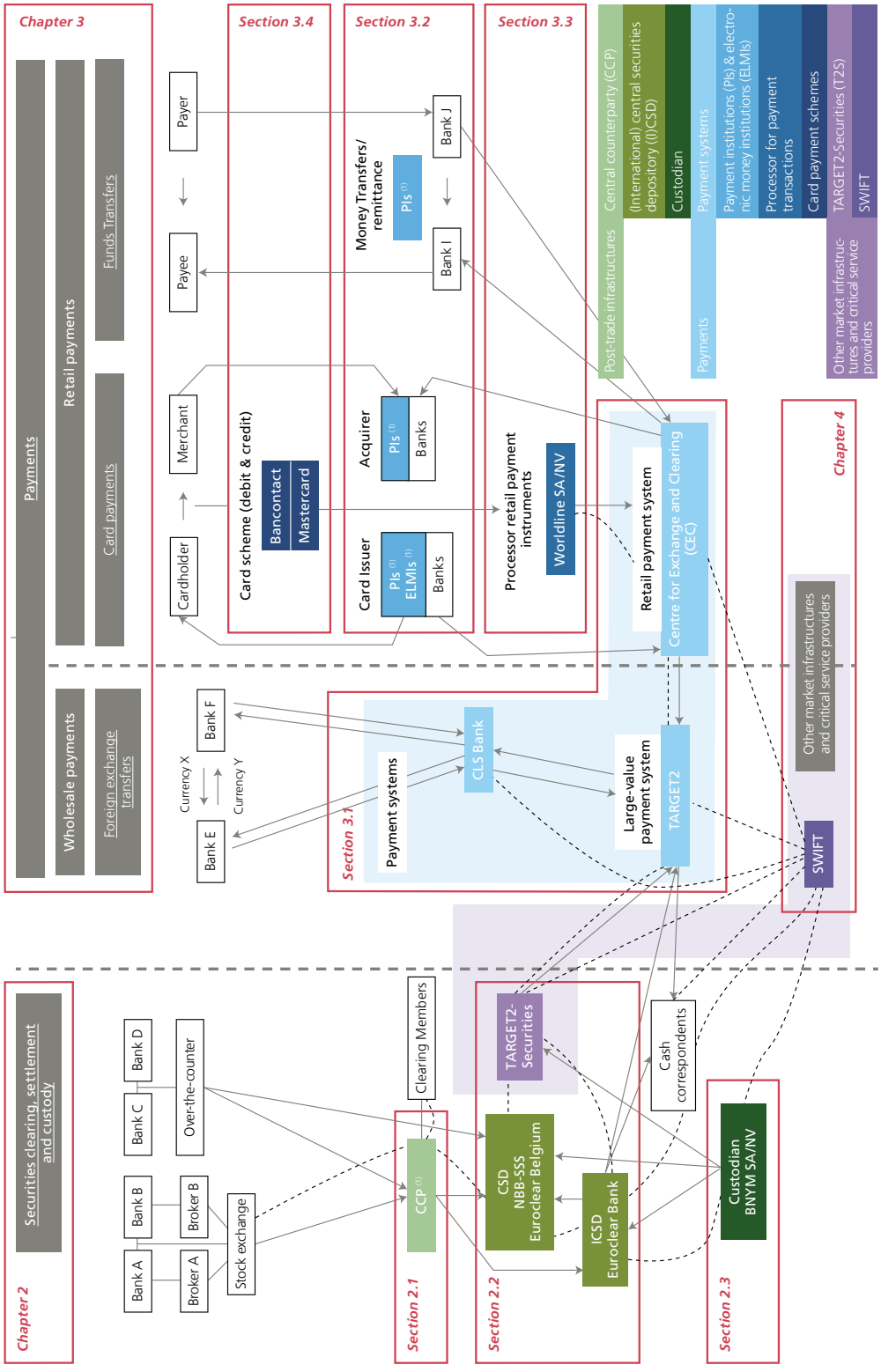
(in %, reference year 2008 as index 0)



Source: NBB calculations.

Chart 1

Interlinkages through & between financial market infrastructures, custodians, payment service providers and other market infrastructures and critical service providers



1 Individual institutions are listed in Table 2

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

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

Oversight and prudential supervision of FMIs differ in a number of areas, ranging from the object of the function, the authority being responsible, the topics covered, as well as the regulatory framework and tools used. However, both oversight and prudential supervision activities, and the framework they are relying on, evolve over time.

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

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

The Bank is also prudential supervisory authority for individual financial institutions, as well as custodians and PSPs like PIs and ELMIs. As of November 2013, a substantial part of the Bank's prudential responsibilities for credit institutions were transferred to the ECB under the Single Supervisory Mechanism (SSM) Regulation[2]. Significant institutions, such as Bank of New York Mellon SA/NV (BNYM SA/NV), are directly supervised by the SSM. Less significant institutions remain under the prudential supervision of the Bank as national competent authority.

Some FMIs are subject to both oversight and prudential bank supervision, typically if the FMI operator has a bank status (as is the case for Euroclear Bank). The oversight activity and prudential supervision are, in such situations, complementary in nature: while the oversight activity focuses on the sound functioning of the settlement system (by assessing compliance with oversight standards such as the 2012 CPMI-IOSCO Principles for FMIs (PFMIs)), the prudential supervision focusses on the financial soundness of the operator (by assessing compliance with banking regulations). As a result, oversight and prudential supervision typically cover different topics. One of the main priorities of oversight relates to the prohibition and containment of any transmission between participants of financial or operational risks through an FMI or service provider. Typical areas oversight is focussing on cover the functioning of the system and how its organisation and functioning minimises or avoids risks not only for itself but – just as importantly – for its participants. Examples thereof include settlement finality rules reducing risks linked to the insolvency of participants (which prevent automatic unwinding of other participants' previous transactions with a bankrupt participant), delivery versus payment (DVP) or payment versus payment (PVP) mechanisms eliminating principal risks in transactions between participants, fair and open access for participants, and stringent requirements on business continuity plans ensuring continuity of services for participants. Oversight also takes into account risks related to system interdependencies (either via connected systems or participants) that could provoke contagion risks in financial markets. Prudential supervision intends

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

2 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).

to ensure that institutions are financially robust at micro-prudential level, thus helping to maintain the trust of the institution's counterparties and, in this way, promoting financial stability. Some types of risks are within focus of both FMI overseers and bank supervisors. However, their perspective is different as an FMI's business model is based on transferring liquidity (which has an element of time criticality) between – or on behalf of – its participants, whereas a bank's business model is rather based on maturity transformation (short term deposits, long term assets). Therefore, the regulatory approach for credit, liquidity and operational risk for FMIs and banks is different. Table 1 compares the different approaches between the oversight of FMIs and the prudential supervision of banks, further illustrated by Chart 2.

As a consequence of such divergences in scope, oversight and prudential supervision are relying on different frameworks. For oversight, the PFMIs cover payment systems, securities settlement systems, CSDs, CCPs and trade repositories. For the implementation of these principles, further clarity is provided by relevant guidelines such as the CPMI-IOSCO guidance on cyber resilience for FMIs or the guidance on resilience and recovery of CCPs. In addition, the CPMI has also published an analytical framework for distributed ledger technology in payment, clearing and settlement.

The tools to conduct oversight and prudential supervision may differ too. Oversight is generally based on principles and guidelines designed in international fora (Eurosystem, CPMI, CPMI-IOSCO). The traditional approach for enforcing them was to urge FMIs and other (critical) service providers to adhering to them via central bank moral suasion (so-called "soft law" approach). Prudential supervision on the other hand, has laid down its requirements in a formal legal framework enacted through EU Directives, Regulations and local laws ("hard law" approach). However, central bank oversight has become more formal, owing to the expanding role

Table 1

Oversight of FMIs and prudential supervision of banks: a different approach

	Oversight of FMIs	Prudential supervision of banks
Authority	Central bank	Supervisory agency or central bank
Scope & objective	Safety and efficiency of payment, clearing and settlement systems (systemic stability)	Financial soundness of banks
Frameworks	CPMI-IOSCO Principles for FMIs (PFMIs) and additional guidance, Eurosystem Oversight Framework	Banking regulations (CRD IV, CRR, Belgian banking law)
Tools and instruments	Moral suasion ("soft law" approach) but in some cases regulation (i.e. PFMIs transposed into hard law by SIPSR, EMIR and CSDR)	Directives/Regulation ("hard law" approach)
Selected examples of attention points	▪ System functioning (settlement finality/efficiency, DVP/PVP, settlement asset, access criteria / default management) ▪ Transmission of risks (between participants or FMIs and critical service providers) ▪ Credit risk: full collateralisation of intraday credit risk ▪ Liquidity risk: intraday dimension and end-of-day balances – cover failure of two largest liquidity exposures ▪ Operational risk: resilience, 2h recovery time objective (2hRTO)	▪ Balance sheet management ▪ Supervisory Review and Evaluation Process (SREP) ▪ Credit risk: end-of-day risk – capital charges on Risk Weighted Assets (RWA) ▪ Liquidity risk: end-of-day risk – liquidity coverage ratio (LCR), net stable funding ratio (NSFR) ▪ Operational risk: capital charges

of the private sector in providing payment and settlement systems, as well as the growing criticality of these systems' proper functioning. In a growing number of cases, oversight is evolving into a hard law approach as illustrated, for example, by the fact that the ECB has laid down its expectations in the ECB Regulation on oversight requirements for systemically important payment systems (SIPSR), or by the 2017 Belgian law on systemically relevant processors for payment transactions. Also, the EU transposed the oversight framework for CCPs and CSDs (i.e. PFMIs) through Regulations (EMIR, CSDR). The Bank has been assigned as the competent supervisory authority for Belgian (I)CSDs, and is, as overseer, also considered as relevant authority under CSDR[1].

Worldline SA/NV is also subject to both prudential supervision (as PI) and oversight (as processor of payment transactions). In order to pool expertise and reinforce the synergies between the oversight function and that of prudential supervision on FMIs, custodians, PSPs and other (critical) service providers, these two functions have been integrated into the same department within the Bank to ensure that its prudential supervision and oversight approach are aligned.

Chart 2

Oversight of FMIs and prudential supervision of banks: illustration of a different approach

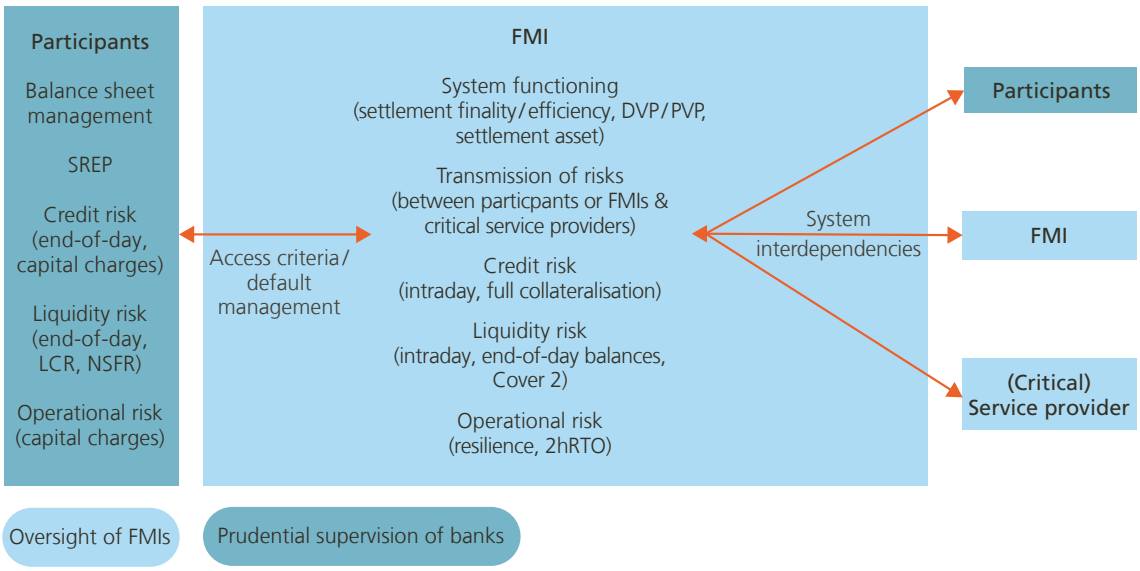


Table 2 below provides an overview of the systems and institutions supervised and/or overseen by the Bank. In addition to the type of services provided, they have been further grouped according to: (i) the type of regulatory role of the Bank (i.e. prudential supervisor, overseer or both) and (ii) the system/institution's international dimension (the Bank as solo authority, international cooperative arrangement with the Bank as lead or in another role). For the systems and institutions established in Belgium which are systemically relevant in other jurisdictions' financial markets or for the financial industry as a whole, the Bank has established cooperative arrangements with other authorities[2]. This may involve multilateral cooperative arrangements, in which the Bank acts as lead overseer (Euroclear, SWIFT). The Bank also takes part in a number of international cooperative

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

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

arrangements (CCPs, BNYM SA/NV, TARGET2, TARGET2-Securities and CLS) in which another national authority acts as lead overseer/supervisor. Domestically, the Bank cooperates with the FSMA which has responsibilities in the supervision of financial markets with regard to conduct of business rules. Annex 2 illustrates the organisation structure of FMIs with an international dimension established in Belgium.

In 2018, the Bank set up TIBER-BE, a framework for testing the cyber resistance of financial institutions and FMIs through controlled ethical hackings. More details are provided in Box 2.

BOX 2

TIBER-BE

Successful cyberattacks can have a major impact on the confidentiality, availability and integrity of payment and securities transactions. Financial institutions and FMIs already carry out regular penetration and other cyber resilience tests by hiring specialized firms to launch short-term targeted tests on various digital parts of an institution. These tests are limited in scope and happen in the test environment. In 2018, the Bank set up a framework that goes a step further than the classic penetration tests; i.e. TIBER or Threat Intelligence Based Ethical Red teaming. This framework, agreed by the Eurosystem, focuses on advanced cyberattacks by organized crime and hostile states, with realistic and customized scenarios based on current threat information and is done in the production environment. TIBER-BE[1] will be rolled out in the course of 2019.

The Bank will work together with experts from the public and private sectors. Tests will be carried out in all discretion, with the help of specialized service providers, and coordinated by the TIBER-BE team. A team of hackers from reputable cybersecurity companies (the so-called "red team") gets the assignment, based on concrete threats, to break into a financial institution or infrastructure, where only a small group (the so-called "white team") knows about the attack. The rest of the organization (the "blue team") must track down, repel and disable the attack without knowing that they are part of a test. The supervisors and/or overseers of the institution concerned do not know in advance of the test either.

The generic test results are shared with the TIBER National Implementation Committee, which includes governmental institutions, critical FMIs and financial institutions. In addition, threat intelligence information is shared within the sector and best practices regarding cyber resilience are developed.

With TIBER-BE, the Bank acts neither in its oversight nor supervisor capabilities but as a catalyst in line with its financial stability mandate. It has established a separate TIBER-BE administrative unit within the service of Surveillance of financial market infrastructures, payment services and cyber risks.

1 https://www.nbb.be/en/payments-and-securities/tiber-be-framework.

Table 2

The Bank's oversight and prudential supervision of financial market infrastructures, custodians, payment service providers and other market infrastructures and critical service providers

(as of April 2019)

	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/NV	Custodian BNYM Brussels branch
			Payment Service Providers (PSPs) Payment Institutions (PIs) *Card acquiring and processing*: *Alpha Card, Alpha Card Merchant Services, Airplus International, Worldline, Lufthansa Airplus ServiceKarten, SIX Payment Services* *Money Remittance*: *Belmoney Transfert, Gold Commodities Forex, HomeSend, Money International, MoneyTrans Payment Services, Travelex, WorldRemit, Transferwise Europe, Moneygram* *Direct Debit*: *EPBF* *Hybrid*: *BMCE EuroServices, Cofidis, eDebex, IBanFirst, Oonex, PAY-NXT, Santander CF Benelux, Ebury, Digtest, Cashfree* *Account Information Services and Payment Initiation Services* *Isabel, Let's DvdVd, Accountable* Electronic Money Institutions (ELMIs) *Buy Way Personal Finance, Fimaser, HPME, Imagor, Ingenico Financial Solutions, Ingenico Payment Services, Viva Payment Services, Paynovate*
Prudential supervision and oversight	CSD Euroclear Belgium (ESES) ICSD Euroclear Bank SA/NV	CCP LCH Ltd (UK), ICE Clear Europe (UK) LCH SA (FR), Eurex Clearing AG (DE), EuroCCP (NL), Keler CCP (HU), CC&G (IT)	
	Assimilated settlement institution Euroclear SA/NV (ESA)		Processor for payment transactions Worldline SA/NV
Oversight	Critical service provider SWIFT	Market infrastructure TARGET2-Securities (T2S)[1]	CSD NBB-SSS
		Payment system TARGET2 (T2)[1] CLS Bank	Card payment schemes Bancontact[1] MasterCard Europe
			Payment system Centre for Exchange and Clearing (CEC)[1]

Post-trade infrastructures	Securities clearing	Payments	Payment systems
	Securities settlement		Payment institutions and electronic money institutions
	Custody		Processor for payment transactions
Other market infrastructures and critical service providers	T2S		Card payment schemes
	SWIFT		

Source: NBB.

1 Peer review in Eurosystem/ESCB.

2. Securities clearing, settlement and custody

FMIs and financial institutions that provide securities clearing, settlement and custody services are considered part of the post-trade securities landscape. Systems that clear trades conducted on a stock exchange or concluded between counterparties on the OTC market, as well as the systems that settle the obligations of the buyer and seller of a trade are subject to oversight. In the EU, institutions that operate these systems are subject to EMIR and CSDR supervision. Chart 3 depicts the scope of the Bank's oversight and supervision role in this area.

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

(I)CSDs, responsible for the last stage in the post-trade chain, are dealt with in section 2.2. Of the three (I)CSDs that Belgium hosts, only Euroclear Bank has banking status and falls under the prudential authority of the ECB. However, as an LSI under the SSM, it remains under the direct prudential supervision of the Bank.

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

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

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

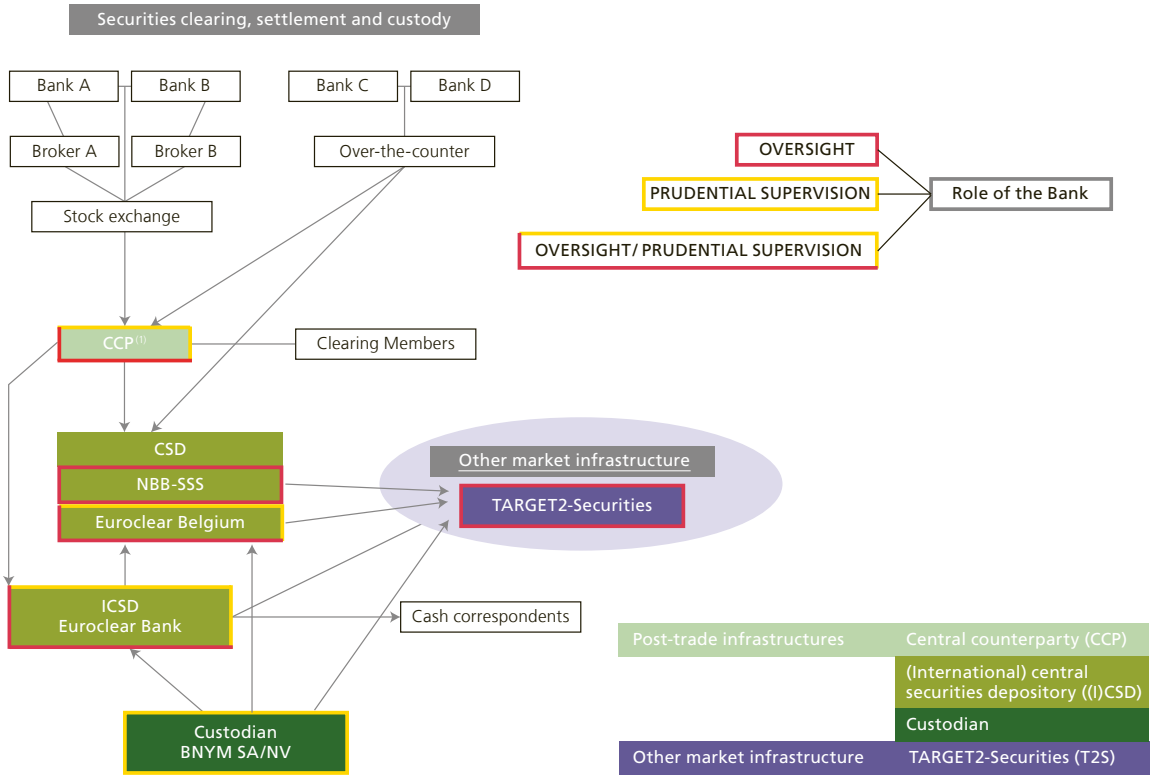
Daily settlement operations of Euroclear Belgium and NBB-SSS are outsourced to TARGET2-Securities (T2S), as in the case of other CSDs in Europe. T2S is not a CSD, but as it provides settlement services to many euro area and some non-euro area CSDs, it is essential that it enables member CSDs to comply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

management framework), as well as the services it provides against an applicable subset of the PFMIs. The Bank is involved in the cooperative oversight of T2S[1].

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

Chart 3

Scope of the Bank's oversight and prudential supervision role in the 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).

2.1 CCPs

Changes in regulatory framework

With the introduction of the clearing obligation – that is, the mandatory use of a central counterparty (CCP) – for standardised over-the-counter derivatives contracts[2], CCPs have become increasingly critical components of

1 Oversight activities of the Eurosystem on T2S are covered in the Eurosystem's Oversight Report. https://www.ecb.europa.eu/paym/pol/html/index.en.html.

2 The clearing obligation is being implemented since mid-2016. It covers standardised interest rate swap contracts in the most relevant currencies, and index-linked credit default swaps. ESMA holds a "Public register for the clearing obligation under EMIR" available on its website at https://www.esma.europa.eu/regulation/post-trading/otc-derivatives-and-clearing-obligation.

the financial system. Back in 2015, the Financial Stability Board (FSB) had set out a workplan to strengthen CCP resilience, and ultimately, its resolvability if need be[1]. This workplan to strengthen the requirements for CCPs is almost fully implemented with the exception of a last aspect related to resolution.

In mid-2017, the FSB published guidance on CCP resolution[2] that covers the required powers for the CCP resolution authority to maintain continuity of critical CCP functions, the use of loss allocation tools and the establishment of crisis management groups for relevant CCPs to ensure adequate cross-border cooperation between authorities. To finalise this work, the FSB consulted[3] the market in November 2018 on two specific aspects, i.e. the availability of financial resources for CCP resolution and the treatment of CCP equity in resolution. The consultation findings will be supplemented with input from existing CCP crisis management groups on current or planned practices for CCP resolution. The final guidance should be available by the end of 2020.

In the EU, EMIR and its Implementing Regulations set out the clearing and reporting obligations for market participants' clearing derivatives, besides the requirements for CCPs and their supervision. In February 2019, the European Parliament, Council of Ministers and Commission reached a preliminary agreement on the so-called EMIR Refit legislation[4] that seeks to relieve small companies – especially non-financial counterparties – of disproportionate costs and administrative burdens, notably by simplifying the requirements relating to reporting and the clearing obligations.

Also in mid-2017, the Commission put forward proposals to improve consistency of supervisory arrangements for CCPs established in the EU, and enhance the EU's ability to monitor, identify and mitigate third-country CCP risks[5]. The Commission, Parliament and Council reached an agreement on EMIR 2.2, i.e. the adaptation of EMIR, in March 2019. The supervision of CCPs will be further harmonised across the EU, while the primary role of CCPs' national competent authority is maintained. EU supervision of CCPs will include wider mandatory consultation of ESMA and an enhanced role for the CCP supervisory college. Issuing central banks for EU currencies are also to be given a bigger role, as regards CCP payment and settlement arrangements, and liquidity risk management. Furthermore, the legislation sets up a direct ESMA supervisory regime for systemic third-country CCPs, and introduces the possibility to require – via a Delegated Act – relocation of so-called "substantially systemically important" CCP activities to the EU. Thus, this legislation prepares for the impact of Brexit in this field by strengthening the third-country CCP authorisation and supervisory regime.

Anticipating the risk of a hard Brexit, ESMA has also given the UK CCPs temporary and conditional recognition as third-country counterparties under EMIR. Without this arrangement, these CCPs would lose their authorisation as an EU CCP overnight, yet they are widely used by EU-based credit institutions that clear in these CCPs and which need to guarantee continuity of their contracts. To avoid market distortions, ESMA has recognised the UK CCPs until 30 March 2020[6].

At the end of 2016, the Commission tabled a proposal for a Regulation on EU CCP recovery and resolution frameworks to ensure the continuity of a CCP's critical functions while avoiding the use of taxpayers' money to restructure and resolve the CCP. The legislative work was put on hold, awaiting the agreement on CCP supervision in EMIR 2.2 as the allocation to EU and national authorities of fiscal responsibility for CCP resolution should mirror the division of tasks of CCP supervision. The Council resumed discussions in May 2019.

1 http://www.fsb.org/2015/09/2015-ccp-workplan/.

2 http://www.fsb.org/2017/07/guidance-on-central-counterparty-resolution-and-resolution-planning-2/.

3 http://www.fsb.org/2018/11/financial-resources-to-support-ccp-resolution-and-the-treatment-of-ccp-equity-in-resolution/.

4 http://europa.eu/rapid/press-release_IP-19-848_en.htm.

5 The Commission's legislative proposal is available at http://europa.eu/rapid/press-release_IP-17-1568_en.htm.

6 The ESMA decision was based on the equivalence decision of the Commission in December 2018 stating that the UK regulatory and supervisory framework for CCPs is equivalent to that of the Union. See Commission Implementing Regulation 2018/2031 of 19 December 2018. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018D2031&from=EN.

Prudential and oversight approach

From a microprudential perspective, the most relevant financial risks faced by a CCP are counterparty risk and liquidity risk if a clearing member defaults. To cope with these risks, a CCP is required by EMIR to be able to withstand at all times the simultaneous default of its two biggest clearing members in extreme but plausible markets, and have adequate resources to cover the losses or to raise the liquidity needed in time. When handling the default of a clearing member, the CCP standardly re-establishes a balanced book via auctioning the positions of the defaulter to surviving clearing members. The adequacy of pre-funded resources and the auction process did get additional attention from supervisors and regulators in the wake of the NasdaqClearing clearing member default in September 2018[1]. CPMI and IOSCO are preparing a market consultation paper in this respect.

In April 2018, ESMA published the framework of its third supervisory stress test for EU CCPs. These tests focus on both the counterparty credit risks and the liquidity risks which CCPs would face as a result of multiple clearing member defaults and simultaneous market price shocks. For this test, new components were added, to assess the impact of liquidation costs for concentrated positions[2].

There is currently no CCP established in Belgium. However, CCPs are relevant for Belgian markets and clearing members, and settle in Belgian (I)CSDs. The Bank continues to participate in seven EU CCP supervisory colleges as listed in table 3. Relevant CCPs include Eurex Clearing AG in Frankfurt, LCH Ltd in London – which clears interest rate swaps in euro and other currencies – and LCH SA in Paris which clears the Euronext Brussels markets. All three CCPs clear repos. Since the end of 2018, euro repo clearing activity has shifted from the London CCP LCH Ltd to its continental partner clearing house LCH SA in Paris. The impact on the clearing of the repo market in Belgian government bonds is shown in Box 3. For volume data on these three CCPs, see also Annex 3.

Supervisory priorities in 2019

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

Based on the FSB guidance, national competent authorities are continuing to set up cross-border crisis management groups for CCP resolution and starting or continuing to plan for CCP resolution. In parallel, based on the CPMI-IOSCO guidance requirements, CCPs are enhancing their recovery rules that stipulate how to allocate default losses to stakeholders, including clearing members. Another continuing priority is the CCP's operational risk management, and in particular the cyber risk it incurs.

In 2018, ESMA issued guidance on CCP conflict of interest management[3] and on anti-procyclicality margin measures for CCPs[4]. National competent authorities are expected to follow up their implementation.

Finally, new services and products, or significant risk model changes implemented by an EU CCP have to be approved by its national competent authority, taking into account the opinion of the CCP's supervisory college.

1 Finansinspectionen describes the event in its November 2018 Stability in the Financial System report (p. 19), available at https://www.fi.se/contentassets/86382ed610304769b77c5a35aa54891f/stability-financial-system-2018-2nn.pdf

2 The ESMA press release on the third EU wide CCP stress test can be found at https://www.esma.europa.eu/press-news/esma-news/esma-launches-third-eu-wide-ccp-stress-test.

3 https://www.esma.europa.eu/sites/default/files/library/esma70-151-1094_final_report_with_guidelines_on_ccps_management_of_conflicts_of_interest.pdf

4 https://www.esma.europa.eu/sites/default/files/library/esma70-151-1293_final_report_on_guidelines_on_ccp_apc_margin_measures.pdf

Table 3

EU CCP supervisory colleges with the Bank's participation

CCP[1]	Main clearing services and relevance for Belgium	Direct Belgian clearing members[2]	EMIR criteria for the Bank's participation in the CCP's supervisory college	
			Supervisor of Belgian clearing members contributing – on a country-by-country basis – most to the CCP default fund	CCP settles in a Belgian (I)CSD[3]
LCH Ltd (UK)	Interest rate swaps/repos	4 ■ AXA Bank Belgium ■ Belfius Bank; ■ BNP Paribas Fortis; ■ KBC Bank		X (EB, NBB-SSS)
Eurex Clearing AG (DE)	Listed interest derivatives/repos	4 ■ Belfius Bank; ■ MeDirect Bank; ■ BNP Paribas Fortis; ■ KBC Bank		X (EB)
LCH SA (FR)	Euronext cash and derivatives trades (including Euronext Brussels) / repos	8 ■ Axa Bank Belgium ■ Banque Degroof Petercam; ■ Belfius Bank; ■ BNP Paribas Fortis; ■ Delen Private Bank; ■ KBC Bank ■ Leleux Associated Brokers; ■ Van De Put & Co Private Bankers		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 EU CCP supervisory college participation is reassessed annually on the basis of the criteria set out in Art. 18 of EMIR. It is worth noting that EMIR 2.2 also makes provision for a third-country CCP supervisory college to be set up.

2 A Belgian bank not mentioned in the table may clear in a CCP but as an indirect clearing member, that is, as the client of a clearing member.

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

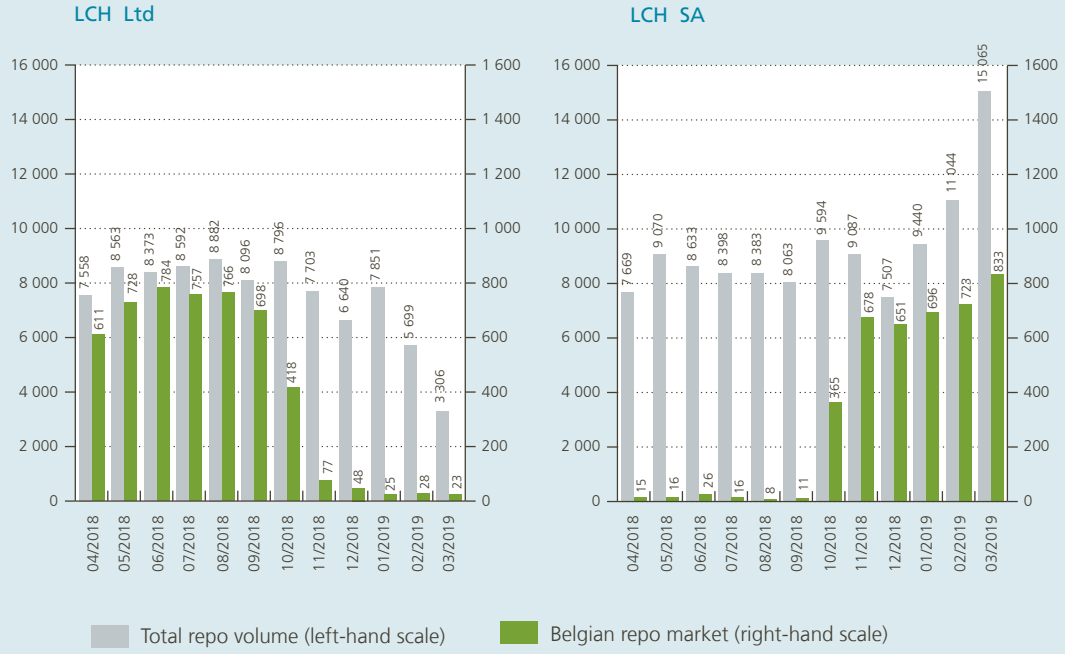
BOX 3

Clearing of repo trades in Belgian fixed-income bonds

After consultation with the market, the London clearing house LCH Ltd started shifting, as from the end of 2018, its clearing business in euro repos to Paris-based LCH SA to accommodate strong demand for migration of euro repo clearing in the euro area. The Belgian repo market – based on OLOs and Belgian Treasury certificates – was one of the first to move to LCH SA. As illustrated in the chart below, this had an impact on the clearing process of the Belgian repo market (representing about € 40 billion per day on average in March 2019). Other euro repo markets (such as Germany, Austria and the Netherlands) followed in the first quarter of 2019. As a result, total repo volumes in LCH SA almost doubled compared to the previous year. From a financial stability point of view, it means that this activity is now being processed by an institution established in the eurozone that has access to central bank services in euro. This is of particular importance for liquidity-intensive activities such as the repo market.

Changes in repo volumes in LCH Ltd and SA and Belgian repo market

(in € billion, total monthly nominal[1])



Source: LCH Ltd and SA.

1 "Nominal" is the sum of contracts' bond nominal value cleared (double-counted).

2.2 (I)CSDs

Changes in regulatory framework

The Commission issued in May 2018 a set of regulatory technical standards on settlement discipline[1]. This Regulation specifies measures to *prevent* settlement fails (including requirements both for investment firms on communications with their clients on trades to be settled and for CSDs to limit the number of settlement fails by providing systems to support matching of settlement instructions). In addition, the Regulation also introduces measures to *address* settlement fails by requiring CSDs to establish monitoring systems (i.e. for the number, value and length of settlement fails) and reporting systems (i.e. for reporting settlement fails to the competent authority and for public disclosure). Furthermore, CSDs have to calculate and apply cash penalties to participants whose settlement instructions fail. In case of systematic failure to deliver securities on the intended settlement day, CSDs may decide to suspend such participants. The rules concerning the buy-in process for financial instruments that have not been delivered (within a certain period set) are also further detailed in this Regulation (i.e. buy-in procedures and notifications, calculation and payment of cash compensations should buy-ins fail or not be possible). In this area, CSDs' responsibility is about providing reporting on buy-ins based on information received from the relevant trading venue or the central counterparties (in case of cleared trades) to the relevant competent authorities. Responsibility for the execution of buy-ins however, remains at the trading level and with the trading parties. The Regulation on settlement discipline will enter into force two years after its publication in the Official Journal of the EU.

In December 2018, ESMA published two consultation papers related to settlement discipline, i.e. guidelines on standardised procedures and messaging protocols used between investment firms and their professional clients to limit the number of settlement fails (under Article 6(2) of the CSDR) and guidelines on the scope, reporting architecture and exchange of information between ESMA and national competent authorities regarding settlement fails, based on the reports submitted by CSDs (following Art. 7(1) of the CSDR). The aim is to finalise both guidelines in Q3 2019. For a consistent and uniform implementation across EU jurisdictions of the 2014 CSDR and the regulatory technical standards, ESMA also continues to update its Questions and Answers section regarding the implementation of the CSDR[2].

On Brexit, by the absence of approval of the Withdrawal Agreement[3], the Commission published in December 2018 a "no-deal" Contingency Action Plan[4]. Precautionary measures were taken to ensure that payments and transfers of securities made by EU participants into UK systems would – in all scenarios – be protected in line with the Settlement Finality Directive.

Following the new regulatory framework in the UK (that is based on the CSDR), EU-based CSDs providing CSD services in the UK will need to apply for recognition in the UK after the UK's withdrawal from the EU takes effect. Such recognition would be required if the CSD has a branch in the UK, settles securities under UK law and has either UK issuers or UK participants. Until they obtain their UK licence, such CSDs would however benefit from a transitional regime (cf. EU CSDR rules for third-country CSDs). In case the CSD would not have its CSDR licence yet, and would still operate under local law, the UK authorities would need to conduct an equivalence assessment of that local law. Both Euroclear Bank and Euroclear Belgium have requested recognition in the UK

1 Regulation (EU) 2018/1229 of 25 May 2018 supplementing Regulation (EU) No 909/2014 of the European Parliament and of the Council with regard to regulatory technical standards on settlement discipline, OJ L 230, 13.9.2018.

2 https://www.esma.europa.eu/press-news/esma-news/esma-updates-its-csdr-qas-0.

3 The Withdrawal Agreement between the EU and the UK of November 2018 stipulated that Union law would still apply in the UK during the transition period (as from March 2019 until the end of 2020, but extendable once by up to one or two years). As the UK would be considered as if it were still an EU country, applicable rules would remain unchanged, including the CSDR. Neither EU nor UK CSDs would therefore be considered as third-country CSDs until the end of 2020.

4 In this Contingency Action Plan, the European Commission provided an equivalence decision with regard to the regulatory framework applicable to UK CSDs for a fixed, limited period of 24 months to ensure that EU institutions would still be able to use UK systems.

to continue to provide CSD services in the UK. As the share of UK participant or issuer activity is minimal in NBB-SSS, the latter decided not to seek designation as third-country system under UK law[1].

Prudential and oversight approach

The three (I)CSDs established in Belgium have a distinct status, scope and risk profile. The Bank adopts different roles with respect to these (I)CSDs. The Bank is also the lead supervisor of Euroclear SA/NV, the financial holding company owning and providing core services to the Euroclear Group (I)CSDs, including Euroclear Bank and Euroclear Belgium.

For the NBB-SSS, the Bank acts in its capacity as overseer. Although the NBB-SSS is being operated by the Bank and therefore exempted from obtaining a CSDR license, it has to comply with the CSDR requirements. For that purpose, NBB-SSS introduced a CRO function and a specific Risk Committee. The latter's mandate is published on the Bank's website[2].

Euroclear Belgium is subject to the Bank's oversight (based on the PFMIs) and CSDR supervision. The CSDR authorisation process for Euroclear Belgium continued to be a key focus. The Bank considered the updated CSDR file, received end September 2018, as complete and started the authorisation process. As Euroclear Belgium shares a common rule book and settlement platform with the other ESES[3] CSDs, the Bank coordinated its assessment with the French and Dutch competent and relevant authorities[4]. Key in the assessment has been the governance of the Euroclear Group and the role of Euroclear SA/NV as both the owner of and critical service provider to the Euroclear Group (I)CSDs for IT, Legal, Risk management, etc. Following the CSDR, measures were taken to strengthen the autonomy and independence of local entities from Euroclear SA/NV, as well as the monitoring framework for outsourcing and critical service providers' relationships via service level agreements and key performance and risk indicators. For the authorisation of Euroclear Belgium, the Bank also involved the FSMA and the Eurosystem; the latter being a relevant authority due to its role as central bank of issue for the EUR (i.e. the settlement currency in Euroclear Belgium). In April 2019, the Bank granted the CSDR licence to Euroclear Belgium[5].

1 The list of EU CSDs applying for recognition in the UK is available at: https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-market-infrastructure-supervision/interim-list-of-third-country-csd.pdf?la=en&hash=3C6C36895859AD0869E651B849B09967F4CE3F1C.

2 https://www.nbb.be/doc/ti/nbbsss_rcmandate.pdf.

3 Euroclear Settlement of Euronext-zone Securities.

4 FR: BdF, AMF; NL: DNB, AFM.

5 The full list of CSDs authorised under Article 16 of CSDR is available at: https://www.esma.europa.eu/sites/default/files/library/esma70-151-889_csd_register.pdf.

BOX 4

International dimension of Euroclear Bank

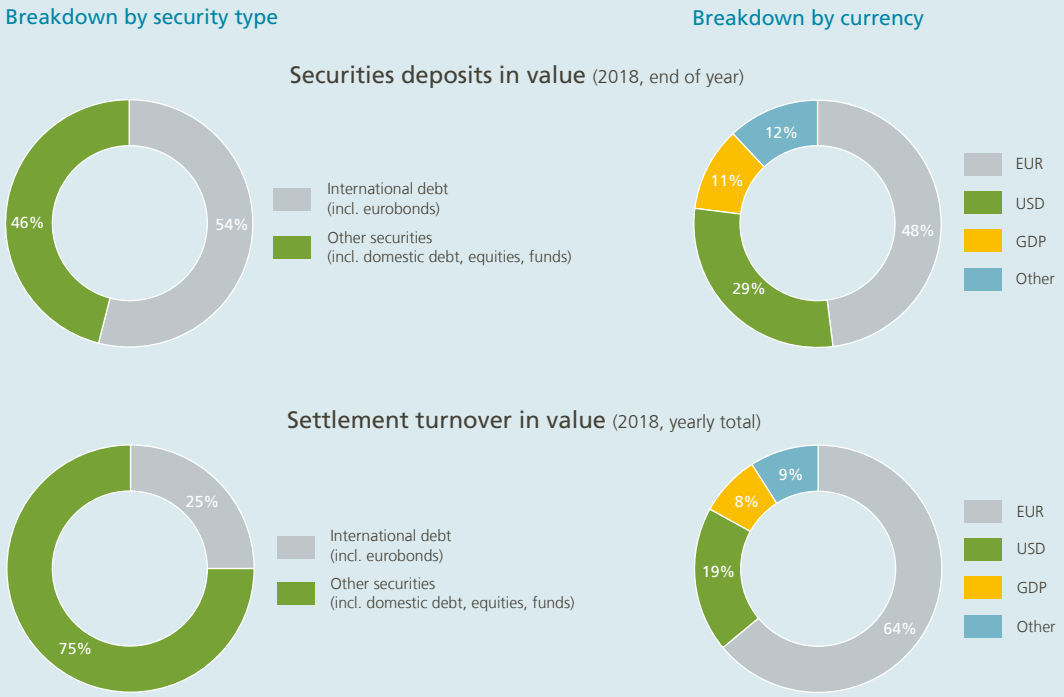
By the very nature of its business model, Euroclear Bank is internationally oriented. This international dimension is reflected in several areas such as participants, currencies and linked securities markets. At the end of 2018, Euroclear Bank had 1 650 participants located worldwide. Its participant base

consists mainly of non-domestic participants, including almost 100 central banks, 27 CCPs and CSDs, as well as credit institutions, broker-dealers and investment banks.

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

To provide services in international bonds and a wide range of foreign securities, about 100 different currencies are eligible in the system operated by Euroclear Bank[1]. Securities can be settled against payment in a Euroclear settlement currency which can be different from the denomination

Securities deposits and settlement turnover in Euroclear Bank



Source: Euroclear.

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

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

currency. Denomination currencies are used as units of account for securities balances but not for payment transactions.

At the end of 2018, the value of securities deposits held on Euroclear Bank's books on behalf of its participants amounted to € 13.5 trillion equivalent (up from € 12.8 trillion in 2017). After EUR (48 %), USD is the main denomination currency (29 %), followed by GBP (11 %). 54 % of securities deposits are in international bonds, such as Eurobonds, for which issuers can choose the currency or country of issue.

Regarding settlement turnover, the number of transactions settled in 2018 in Euroclear Bank amounted to 107.0 million (up from 95.4 million in 2017). In value terms, this represents € 525.7 trillion (up from € 498.1 trillion in 2017). 64 % of settlement turnover, free of payment and against payment transactions, was denominated in EUR, after USD (19 %) and GBP (8 %). In terms of settlement turnover per security type, compared to securities deposits, international debt accounts for 25 % while the bulk is composed of other types of securities such as domestic debt and, to a lesser extent, equities or exchange-traded funds.

The interconnectivity of Euroclear Bank with other FMIs is a critical component in the Euroclear Group strategy to establish a common pool of collateral assets in which Euroclear Group entities provide collateral management services as a triparty agent taking over the collateral management tasks (including collateral selection, valuation and substitution) from its participants during the lifecycle of the transaction concluded between two participants. At the end of 2018, at group level, the average daily value of triparty collateral managed by the Euroclear (I)CSDs reached € 1.224 trillion equivalent (up from € 1.150 trillion in 2017).

The specific international and multicurrency dimension of Euroclear Bank is detailed in Box 4. Euroclear Bank is not only subject to the Bank's oversight and CSDR supervision but also to its prudential bank supervision. See also Box 5 on "Euroclear, Banking Supervision and the SSM" in that regard.

For the CSDR authorisation, Euroclear Bank has to apply not only for a CSD licence but also for a banking licence[1], both including elements of the interoperable link with Clearstream Banking Luxembourg. In the course of 2018, Euroclear Bank implemented several measures relevant for CSDR compliance. As an example, for the interoperable link between Euroclear Bank and Clearstream Luxembourg (the so-called "Bridge"), a solution was implemented jointly by both ICSDs in October 2018 to avoid any unsecured credit exposures due to settlement activity via the Bridge. The Bank also focused on specific liquidity risk management requirements under the CSDR, in particular the "Cover 2" requirement. It implies that Euroclear Bank should have sufficient qualifying liquid resources (QLR) in each relevant currency[2] to meet its payment obligations if the two participants on which Euroclear Bank has the largest liquidity exposure default. To meet this requirement, Euroclear Bank has reviewed relevant aspects of its credit and liquidity risk management framework. It reduced

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

2 Relevant currencies are identified based on, in accordance with EBA RTS Art. 36.8, the most relevant Union currencies as well as their share in the largest net negative liquidity positions of the CSD-banking service provider. However, for a transitional period of 12 months, relevant currencies can be identified based on the relative share of each currency in the total value of against payment settlement.

potential liquidity exposures by further decreasing intraday credit limits on participants and increased the level of its own QLR. The new credit and liquidity risk management framework being implemented by Euroclear Bank is based on a multicurrency ex-ante approach (i.e. limits are set by currency depending on its QLR in that currency) as opposed to an ex-post control framework (i.e. whereby measures are taken by the (I) CSD afterwards based on the outcome of liquidity back-test scenarios). At exposure level, the framework incorporates the different roles participants can have in the system. At QLR level, and in accordance with the CSDR, high-quality collateral pledged by participants that has an active outright sale or repo market and for which reliable access can be demonstrated, including in stressed conditions, or that can be liquidated through a pre-arranged and highly reliable funding arrangement, is included. In that regard, credit limits are based on collateral hierarchy principles imposing minima for best (liquid) collateral and maxima for lower quality collateral. Since the full amount of QLR is not available the whole day due to liquidity facilities' cut-off times or repo market deadlines, credit lines will be reduced towards the end of the day in function of the available QLR. This allows for a dynamic (intraday) credit and liquidity risk management. In addition, long cash balances that participants leave overnight on their cash accounts are not qualified as QLR as these participants have the contractual right to withdraw all these balances in full at any time [1]. These enhancements in Euroclear Bank's liquidity risk management framework were being implemented in Q1 and Q2 of 2019. Further work on "fat-tail risks" scenarios such as procedures to cover unexpected liquidity shortfalls has been conducted in 2019 as well.

In the framework of the PFMIs, the Bank consults and considers the views of the other authorities of the Multilateral Oversight Group (i.e. Federal Reserve, Bank of England, Bank of Japan, and ECB as observer). In this forum, the Bank continued to discuss specific issues in the area of operational risk management (operational and cyber resilience) as well as credit-related risks due to participants' long cash balances and income and redemption pay-in flows. Apart from solving inefficiencies in its processing of such payment flows, one of the strategies of Euroclear Bank to mitigate these risks is to divert incoming payments to central bank accounts. EUR payments are gradually being shifted to Euroclear Bank's TARGET2 account. As of March 2019, Euroclear Bank also became a direct participant of the central bank money cash system of the Bank of England (CHAPS). For that purpose, Euroclear Bank holds a settlement account at the Bank of England allowing the transfer of £ payments.

Cyber resilience also continues to be a priority for the Bank in its oversight activities with Belgian (I)CSDs. Within the Euroclear Group, different projects to further enhance its cyber resilience are ongoing. A Cyber Resilience Task Force, encompassing overseers and supervisors of all group entities and chaired by the Bank, is monitoring the implementation of these projects. End 2018, the Euroclear Group entities self-assessed them as compliant with the mandatory controls of the SWIFT Customer Security Programme which aims to improve the security of the customers' connectivity to the SWIFT network (i.e. end-points of payment and securities settlement systems).

The governance structure of the Euroclear Group has been changed since November 2018. Euroclear plc, the top financial holding established in the UK, has been transferred to Belgium in anticipation of Brexit. Euroclear Holding SA/NV has now become the top financial holding of Euroclear and is – as Euroclear Plc previously – set up as a passive holding. Its activities mainly consists of detaining participations in the financial holding Euroclear SA/NV (indirect) and the other (I)CSD entities of the Group. The new structure of the Euroclear Group is shown in Annex 2. Changes also occurred in Euroclear's shareholdership. In 2018, the US exchanges operator Intercontinental Exchange (ICE) became one of the largest shareholders after having increased its share up to close to 10 %. End 2018, the Federal Holding and Investment Company (SFPI-FPIM) acquired about 2 % of the shares in Euroclear. The London Stock Exchange Group also bought a stake of close to 5 % in early 2019.

1 Whereas in banking regulation, 30 % of "operational balances" could be considered as "stable".

BOX 5

Euroclear, Banking Supervision and the Single Supervisory Mechanism

As of November 2014, the Single Supervisory Mechanism (SSM) entered into force, designating a group of EU banking institutions as Significant Institutions (SIs) and placing them under the direct supervision of the ECB in cooperation with the national competent authorities (NCAs), whereas the NCA remained lead supervisor on the remaining banking institutions, the Less Significant Institutions (LSIs). The decision on whether a bank is deemed an SI is based on several criteria including the size of the balance sheet (> € 30 billion). A yearly significance assessment is performed by the ECB in cooperation with the relevant NCAs to review the list of SIs. Moreover, the ECB can at any time decide to take control of the direct supervision of an LSI if this is justified for the consistent application of its supervisory standards. Euroclear Bank has been classified by the ECB as an LSI as well as Euroclear SA/NV, a financial holding established in Belgium and owner of Euroclear Bank. Both thus remain under the direct banking supervision of the NCA, namely the Bank.

Euroclear SA/NV consolidated and Euroclear Bank standalone have also been designated as Other Systemically Important Institutions (O-SIIs) by the Bank, which means that both are considered as domestically important institutions. O-SIIs are defined as institutions whose failure would have a significant impact on the financial system or the real economy. They need to hold an additional macro-prudential capital buffer on top of the other regulatory capital requirements. These additional buffers have two principal motivations. Firstly, to reduce the probability of default of the institution, given the high economic and social costs of such a default, and secondly, to impose surcharges on the institution that reflect the negative externalities that its failure would generate. The Bank decided that Euroclear SA/NV consolidated and Euroclear Bank standalone must retain an O-SII capital buffer of 0.75 % of its risk weighted assets. The domestic importance of the Belgian-based banks is reassessed on an annual basis by the Bank. The methodology to identify the O-SIIs is published on the Bank's website[1] and considers criteria such as size, complexity, interconnectedness and substitutability.

1 https://www.nbb.be/nl/financieel-toezicht/macroprudentieel-beleid/macroprudentiele-instrumenten/buffer-voor-de-andere.

Supervisory priorities in 2019

After the CSDR authorisation of Euroclear Belgium in April 2019, the priority for 2019 is the authorisation file for Euroclear Bank. Given its international scope and multicurrency dimension, the Bank will consult with a wide range of other relevant and competent authorities in the EU member states in the framework of the CSDR (See Box 6). Further work will also be conducted on the potential use by Euroclear Bank of central bank services for non-EU currencies.

A standing topic on the Bank's supervision and oversight plan continues to be operational resilience and cyber security in the Euroclear Group (i.e. Euroclear SA/NV, Euroclear Bank and Euroclear Belgium), in cooperation with other Euroclear Group regulators in the framework of the Cyber Resilience Task Force.

In addition, the Bank will pay attention to Euroclear corporate governance aspects (such as potential evolutions in the shareholder structure of the Group) and to the impact of Brexit on the Euroclear business and strategy. On the latter, in May 2019, Euroclear Bank published its proposal to become the issuer CSD for Irish corporate securities as from March 2021.

BOX 6

Cooperation between the Bank and other authorities with regard to Euroclear

The Bank cooperates with domestic and foreign authorities in the framework of the oversight and supervision of Euroclear entities established in Belgium, i.e. Euroclear SA/NV, Euroclear Bank and Euroclear Belgium. The table below provides the list of authorities and the rationale for having a cooperation arrangement with them.

In the framework of the CSDR, the Bank, as competent authority, also needs to involve other relevant authorities in the authorisation and supervision of (I)CSDs established in Belgium. The CSDR identifies as "relevant authorities", i.e. authorities responsible for oversight, central banks in the EU in whose books cash is settled and central banks in the EU issuing the most relevant currencies in which settlement takes place. In the case of Euroclear Bank and Euroclear Belgium, the Bank also acts as relevant authority in its role as overseer of securities settlement systems. As Euroclear Belgium settles EUR in central bank money, the Eurosystem (represented by the Bank) is considered as relevant authority as well. For Euroclear Bank, this also includes Bank of England and Danmarks Nationalbank. For this category of relevant authority – central banks in the Union issuing the most relevant currencies in which settlement takes place –, the parameters to assign relevant authorities are defined by the CSDR RTS. As some of these parameters require a calculation of data on an aggregate basis, ESMA collects, via the competent authorities, data across all CSDs. ESMA publicly discloses the list of relevant authorities[1].

In addition, the Bank has to involve other authorities for the authorisation to provide banking-type ancillary services. These include (i) the relevant authorities (as defined in the previous paragraph), (ii) the competent authorities in the Member State (MS) where the CSD has established interoperable links with another CSD, (iii) the competent authorities in the host MS where the activities of the CSD are of substantial importance for the functioning of the securities markets and the protection of investors, and (iv) the competent authorities responsible for the supervision of the participants of the CSD established in the three MS with the largest settlement values in the CSD's securities settlement system.

Given the need to use consistent data aggregated at EU level for the calculation of the respective indicators, ESMA issued guidelines on the data collection, processing and aggregation process to determine (i) the most relevant currencies in which settlement takes place[2] and (ii) the substantial importance of a CSD for a host MS[3].

1 https://www.esma.europa.eu/sites/default/files/library/esma70-151-887_csdr_list_of_relevant_ authorities_ art_12.pdf.
2 https://www.esma.europa.eu/sites/default/files/library/esma70-708036281-66_csdr_guidelines _on_relevant_currencies_0.pdf.
3 https://www.esma.europa.eu/sites/default/files/library/esma70-708036281-67_csdr _guidelines _on_substantial_importance_of_a_csd_0.pdf.

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

Source: NBB.

Consultation in the context of the CSDR	Rationale for consultation
National consultation	
Euroclear Bank / Euroclear Belgium	
CSD services	
FSMA	The Bank seeks the FSMA's advice for aspects that fall under the latter's perimeter of competence for CSDs. This covers rules on conflicts of interest, record-keeping, the requirements concerning participation, transparency, procedures for communicating with participants and other market infrastructures, the protection of the assets of participants and their clients, freedom to issue securities via any CSD authorised in the EU, and access between a CSD and another market infrastructure [1]
International consultation	
Euroclear Bank	
CSD services	*Central bank of issue of the most relevant currencies in which settlement takes place* [2].
Eurosystem, Bank of England, Danmarks Nationalbank	Calculation methodology [3]: ■ the relative share of each Union currency in the total value of the settlement by a CSD of against-payment settlement instructions, provided that such share exceeds 1 %; or ■ the relative share of against-payment settlement instructions settled by a CSD in a Union currency compared to the total value of A/P settlement instructions settled in that currency across all CSDs in the Union, provided that such share exceeds 10 %
Banking-ancillary services	*The following authorities are involved in the authorisation of the CSD* [4]
Eurosystem, Bank of England, Danmarks Nationalbank	■ Relevant authorities
Commission de Surveillance du Secteur Financier (CSSF)	■ Competent authority in the MS where the CSD has established interoperable links with another CSD
Competent authorities from twenty MS in the EU	■ Competent authorities in the host MS where the activities of the CSD are of substantial importance for the functioning of the securities markets and the protection of investors [5] Calculation methodology: the aggregated market value of financial instruments issued by issuers from the host MS that are initially recorded or centrally maintained in the CSD represents at least 15 % of the total value of financial instruments issued by all issuers from the host MS that are initially recorded or centrally maintained in all CSDs established in the Union [6] ■ Competent authorities responsible for the supervision of the participants of the CSD established in the three MS with the largest settlement values in the CSD's securities settlement system on an aggregated basis
ESMA, EBA	■ European regulatory agencies
Euroclear Belgium	
CSD filing	
Eurosystem	Eurosystem (as represented by the Bank) as central bank in the Union in which books cash is settled and issuing the most relevant currency in which settlement takes place

Source: NBB.

1 In accordance with the Protocol between the Bank and the FSMA on their cooperation in the framework of the supervision of CSDs and assimilated institutions.

2 CSDR Art. 12(1)(b).

3 Art. 2(1)(a) of the Commission Delegated Regulation (EU) 2017/392.

4 CSDR Art. 55(4).

5 Art. 24 of Regulation (EU) No 909/2014 (CSDR).

6 Art. 5(1)(a) of the Commission Delegated Regulation (EU) 2017/389.

2.3 Custodians

Changes in regulatory framework

The Law of 31 July 2017 introduced a new licence which can be granted to credit institutions carrying on activities exclusively in the following areas: custody and asset servicing, bookkeeping and settlement in financial instruments, as well as associated services, in addition to accepting deposits or other returnable funds from the public and granting credit for own account, where such activities are ancillary or linked to the above-mentioned services (hereinafter referred to as "depositary banks"). As the banking supervision framework does not address all prudential supervision aspects of this type of activity (e.g. customer asset protection), a specific prudential supervision approach is warranted in areas which are not covered by the banking regulations.

The Bank of New York Mellon SA/NV (BNYM – a Significant Institution according to the SSM Regulation) and The Bank of New York Brussels Branch (BNYM BB) – a third-country branch holding in global custody mainly assets from non-continental EU customers – were granted a complementary licence to operate as depositary banks at the end of 2017 (see also Annex 2 for the governance structure of the BNYM group).

Moreover, other non-bank specific prudential regulation introduced additional reporting requirements for credit institutions. One of them, namely reporting on settlement internalisers within the context of the CSDR, is particularly relevant for institutions providing custody and related services. See Box 7 for more information on settlement internalisers.

BOX 7

New reporting obligation for settlement internalisers

On 23 July 2014 the European Parliament and the Council adopted the European Regulation on improving securities settlement in the EU and on central securities depositories[1] (the "CSDR").

According to Article 9(1) of the CSDR, settlement internalisers shall report to the competent authorities of their location of establishment on a quarterly basis the aggregated volume and value of all securities transactions that they settle outside securities settlement systems.

"Settlement internaliser" means any institution, including those authorised in accordance with Directives 2013/36/EU[2] or 2014/65/EU[3], which settles transfer orders on behalf of customers on its own account rather than through a securities settlement system[4].

The aim is to take further steps for improved transparency and to provide regulators with an extensive view of the securities settlement infrastructure, potentially inducing policy changes to improve safety in the markets.

1 Regulation (EU) No 909/2014.
2 Authorisation for credit institutions to provide services throughout the Union.
3 Authorisation for investment firms to provide services throughout the Union.
4 Art. 2(1)(11) of the CSDR.

Further information on the requirements regarding the content of the reporting on internalised settlements is provided in Commission Delegated Regulation (EU) 2017/391 of 11 November 2016 (hereinafter referred to as the 'RTS'). Technical standards regarding the templates and procedures for the reporting and transmission of information on internalised settlements are specified in Commission Implementing Regulation (EU) 2017/393 of 11 November 2016.

To ensure a common, uniform and consistent application of Article 9 of the CSDR and the relevant provisions of the RTS on internalised settlement, ESMA issued guidelines (28 March 2018) clarifying the scope of the data to be reported by settlement internalisers and the types of transactions and operations that should or should not be included.[1]

All institutions in scope of the reporting requirements should comply with the ESMA Guidelines from the first reporting period onwards. In accordance with Article 1(1) of Commission Implementing Regulation (EU) 2017/393, (i) the period that the first report shall cover goes from 1 April 2019 until 30 June 2019; and (ii) settlement internalisers shall send the first report to the competent authorities by 12 July 2019.

The following types of transactions and operations are considered *in scope* of internalised settlement reporting:

- purchase or sale of securities (including primary market purchases or sales of securities);
- collateral management operations (including triparty collateral management operations or auto-collateralisation operations);
- securities lending or securities borrowing;
- repurchase transactions;
- transfers of securities between accounts of different investment funds (funds with or without legal personality should be treated as customers);
- execution of transfer orders by a settlement internaliser on its own account, to the extent that they result from securities transactions with customers of the settlement internaliser;
- transfer of securities between two securities accounts of the same customer;
- title transfer financial collateral arrangements as defined in point (b) of Article 2(1) of Directive 2002/47/EC (SFD);
- security financial collateral arrangements as defined in point (c) of Article 2(1) of SFD, where there is a transfer of securities between accounts;
- corporate actions on flow represented by transformations.

The following types of transactions and operations are considered *out of scope* of internalised settlement reporting:

- corporate actions on stock, such as cash distributions (e.g. cash dividend, interest payment), securities distributions (e.g. stock dividend, bonus issue), reorganisations (e.g. conversion, stock split, redemption, tender offer);
- corporate actions on flow represented by market claims;
- primary market operations, meaning the process of initial creation of securities;
- creation and redemption of fund units;
- pure cash payments, not related to securities transactions;
- transactions executed on a trading venue and transferred by the trading venue to a CCP for clearing or to a CSD for settlement.

1 ESMA70-151-1258.

The following types of financial instruments should be considered *in scope* of internalised settlement reporting:

- financial instruments that are initially recorded or centrally maintained in CSDs authorised in the EU;
- financial instruments initially recorded and/or centrally maintained outside of CSDs authorised in the EU but settled in a European CSD.

On 5 February 2019, the Bank published[1] a circular to implement the ESMA guidelines of 28 March 2018 on Internalised Settlement Reporting under Article 9 of the CSDR.

1 https://www.nbb.be/doc/cp/eng/2019/20190205_nbb_2019_02.pdf.

Prudential approach

As a Significant Institution, BNYM falls under the direct supervision of the SSM. The majority of planned supervisory actions are therefore carried out jointly by the Bank and the ECB within the SSM framework. BNYM is also subject to specific monitoring by the Bank as regards the specific requirements applicable to depositary banks on *inter alia* the customer asset protection framework and compliance of new activities/acquisitions. As a third-country branch, BNYM BB falls under the direct supervision of the Bank.

BNYM and BNYM BB have a specific business model and consequently a risk profile that is distinct from that of other credit institutions; i.e. their business lines all relate to the investment servicing activity for professional counterparties. They do not engage in retail banking. The liability side of their balance sheet consists predominantly of non-maturity customer deposits. They receive cash deposited by customers to finance their transactions. These customer deposits are reinvested in the market, intragroup, with central banks or in high-quality investment portfolios. Credit granted to customers has an operational, uncommitted nature; i.e. (intraday) overdrafts are granted to facilitate the processing of transactions.

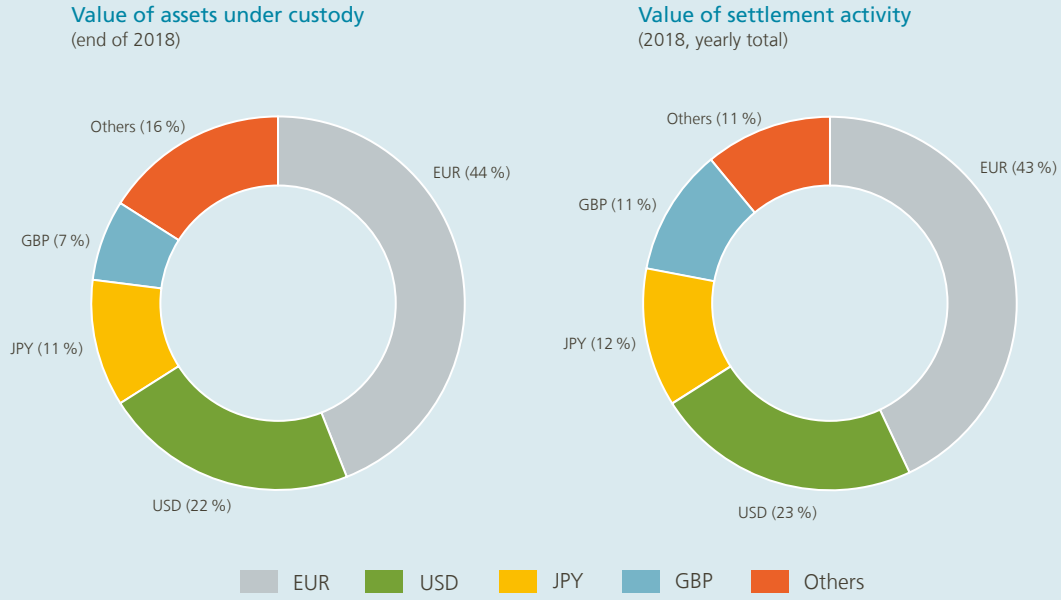
BNYM's activity is largely situated off-balance sheet (€ 2.4 trillion assets under custody as of end 2018) and its profit is mainly fee-driven. Customers are mostly institutional counterparties. This is one of the concentration risks inherent to the custodian business model. As for other custodian banks, the risk profiles of BNYM entities in Belgium are driven by (intraday) credit risk, intraday aspects of liquidity, and operational risk (including IT risks) resulting from tail operational events such as FMI disruptions or failures due to the role of a custodian bank in the settlement process. Acting as a global custodian of the BNYM Group, BNYM has a strong international dimension, as explained in Box 8.

The SSM, which has established a harmonised supervisory approach for banks under its direct supervision, also takes into account the specificities of the business model and risk profile of custodians. An important level of supervisory judgement for custody-specific risks is currently required from the joint supervisory team when supervising SSM custodians, in order to ensure that all material risks for custodian banks are identified and captured in all parts of the SSM supervisory process (such as risk assessment, SREP, stress test and recovery planning).

BOX 8

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

Assets under custody and settlement turnover in BNYM SA/NV by currency



The Bank of New York Mellon, a banking group incorporated in the US, is the largest custody bank in the world in terms of assets under custody ($ 33.1 trillion as at December 2018). It is a global systemically important bank (G-SIB), providing asset and investment management services to institutional customers. The Bank of New York Mellon SA/NV (BNYM), the Belgian subsidiary, provides asset services mainly and acts as the Groups' custodian for T2S markets and as the custodian for EU customers. BNYM has a non-bank subsidiary in Germany and branches in the UK, Luxembourg, the Netherlands, Germany, France, Ireland and Italy, through which it operates in these local markets. BNYM qualifies as an 'other systemically important institution' (O-SII) as assessed by the Bank based on the relevant EBA guidelines.

By the end of 2018, BNYM served more than 2 100 international, institutional customers on whose behalf it held € 2.4 trillion equivalent assets under custody, denominated in more than 75 different currencies[1]. The majority of these assets are denominated in EUR (44 %), followed by USD (22 %), JPY (11 %) and GBP (7 %). In terms of settlement activity[2], BNYM processed about 16.2 million transactions worth 42.2 trillion equivalent in 2018. The main currencies are EUR (43 %), USD (23 %), JPY (12 %) and GBP (11 %).

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

2 Value of BNYM settlement activity is based on receipt and delivery instructions.

Supervisory priorities in 2019

Prudential supervision of BNYM will focus on the impact of Brexit. The withdrawal of the UK from the EU will redesign the regulatory landscape for the BNYM group, impacting both product offering and reliance on intra-group outsourcing to the UK. The ECB has published guidance for prudential supervisors for assessing the impact of Brexit[1]. This guidance revisits principles on governance and risk management, outsourcing, recovery and resolution, booking models, dual hatting, etc. Assuring that BNYM is compliant with these principles and other regulation in this regard will be a priority.

Alongside, but not entirely disconnected from adapting the business model to a post-Brexit environment, BNYM is currently in the process of simplifying its footprint structure in Europe (including the UK). This process entails different strategic initiatives that are changing the way customers are serviced. These include *inter alia* the transfer of activities and customers between group entities. The Bank is closely monitoring these transfers to safeguard customers' interest and assets.

Institutions qualified as settlement internalisers within the meaning of the CSDR need to report to the Bank on a regular basis. In accordance with the applicable Implementing Regulation, they should provide their first report by mid-July 2019. The Bank will monitor compliance with these requirements through its supervisory activities.

1 https://www.bankingsupervision.europa.eu/banking/relocating/html/index.en.html.

3. Payments

The Bank has broad responsibility in the area of payments and adopts the role of both overseer and prudential supervisor, as illustrated in chart 4 below. Oversight focuses on payment systems, instruments[1] and schemes[2] while prudential supervision targets payment service providers (PSPs). These approaches are complementary: while oversight concentrates on the sound and safe functioning of payment systems, payment instruments, payment schemes or other payment infrastructures, supervision pursues safe, stable and secure financial institutions delivering payment services to the end users.

The interest of central banks in the area of payments stems from a connection with various core tasks. Directly or indirectly, payment systems, instruments and services may affect the practical implementation of monetary policy, the financial stability of the country, confidence in the currency, as well as contribute to a safe, reliable and competitive environment.

Section 3.1 covers the two payment systems which are core for the Belgian payment infrastructure: TARGET2 and the Centre for Exchange and Clearing (CEC). TARGET2 is the large-value payment system connecting Belgian banks with other euro area banks for processing payments and serves as the basic connecting infrastructure for the implementation of central bank monetary policy. CEC is the domestic retail payment system (RPS) processing intra-Belgian domestic payments.

The Bank also participates in the cooperative oversight framework of CLS Bank, a US-based payment-versus-payment (PvP) settlement system for foreign exchange (FX) transactions. CLS has been designated as a systemically important financial market utility by the US Financial Stability Oversight Council with the US Federal Reserve Board as the Supervisory Agency. The Federal Reserve Bank of New York supervises CLS under delegated authority from the Federal Reserve Board. In addition, CLS is overseen by the Oversight Committee (OC), an international cooperative oversight arrangement comprised of the central banks whose currencies are settled in CLS and five central banks from the euro area (including the Bank), with the US Federal Reserve acting as lead overseer and performing the secretariat function for the OC.

Prudential supervision of Payment Institutions (PIs) and Electronic Money Institutions (ELMIs) – a relatively new sector of PSPs which may offer since 2009, just like banks, payment services in Europe – is described in section 3.2. This category of non-bank PSPs for retail payments provides respectively payment services and the issuing, redeeming and distributing of electronic money. ELMIs may also provide payment services and, given their ability to issue electronic money to the public, are subject to a stricter prudential regime, such as stronger capital requirements.

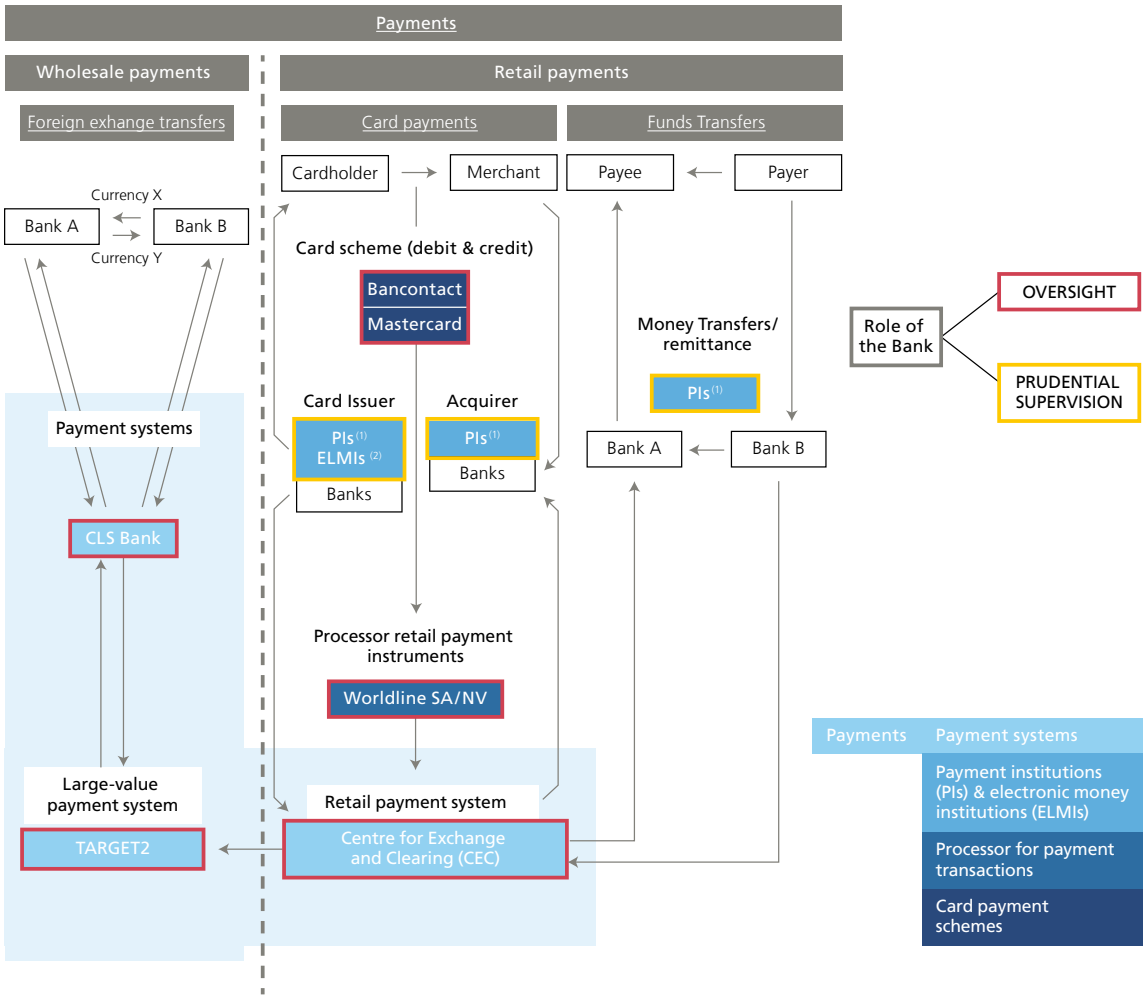
As acquirer[3] and processor of payment transactions in Belgium, Worldline SA/NV is subject to both prudential supervision and oversight. The Bank's activities in that respect are covered in section 3.3.

1 A payment instrument is an instrument to execute payments such as cards, credit transfers and direct debits.
2 A payment scheme is a set of rules, practices, standards and/or guidelines for the execution of payment transactions.
3 Acquiring of card payments is the service whereby a payment service provider contracts with a payee (merchant) to accept and process payment transactions, and guarantees the transfer of funds to the payee (merchant). The processing part is often performed by another entity.

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

Chart 4

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



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

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

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

3.1 Payment systems

Changes in regulatory framework

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

Oversight approach

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

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

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

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

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

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

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

BOX 9

Instant Payments

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

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

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

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

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

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

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

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

Supervisory priorities in 2019

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

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

3.2 Payment institutions and electronic money institutions

Changes in regulatory framework

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

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

1 The Law of 11 March 2018 on the legal status and supervision of payment institutions and electronic money institutions, access to the payment service provider's business and the issuing of electronic money activity, and access to payment systems (publication in the Belgian Official Gazette of 26 March 2018).

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

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

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

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

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

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

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

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

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

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

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

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

Prudential approach

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

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

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

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

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

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

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

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

5 Ebury, Moneygram, Transferwise Europe and WorldRemit.

6 Africash, Instele, and Rent A Terminal Belgium.

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

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

BOX 10

Money remittance in Belgium

Money remittance is defined in the Payment Services Directive (PSD2) as "a payment service where funds are received from a payer, without any payment accounts being created in the name of the payer or the payee, for the sole purpose of transferring a corresponding amount to a payee or to another payment service provider acting on behalf of the payee, and/or where such funds are received on behalf of and made available to the payee".

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

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

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

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

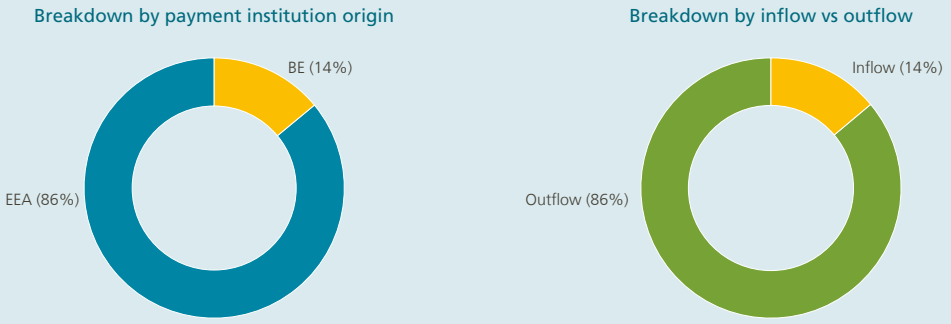
Taking into account both incoming and outgoing money transfer flows, Morocco (21 %), Romania (10 %) and Turkey (9 %) remain the most important countries for the money remittance business taking place in Belgium in value terms (chart 2, left-hand panel). By number of transactions, Morocco (39 %), the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

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

Overview of money remittance in Belgium

Chart 1 – Money transfers by payment institutions present in Belgium

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



Money transfers by all money remitters present in Belgium

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

Chart 2 – Top-10 Country Corridors

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

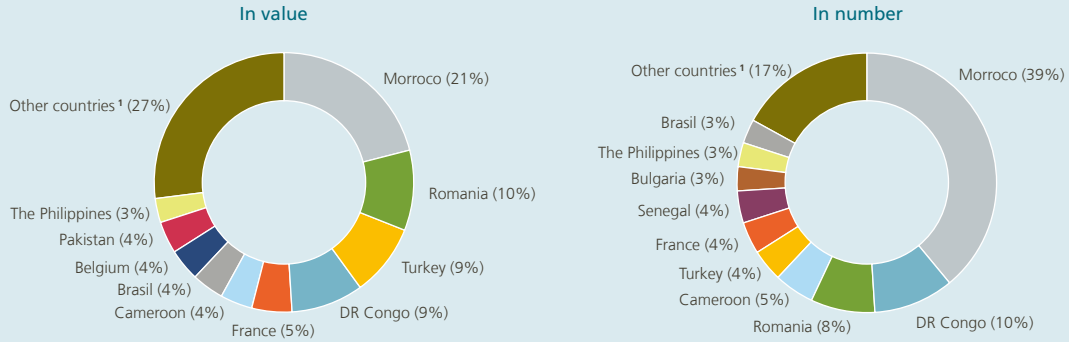
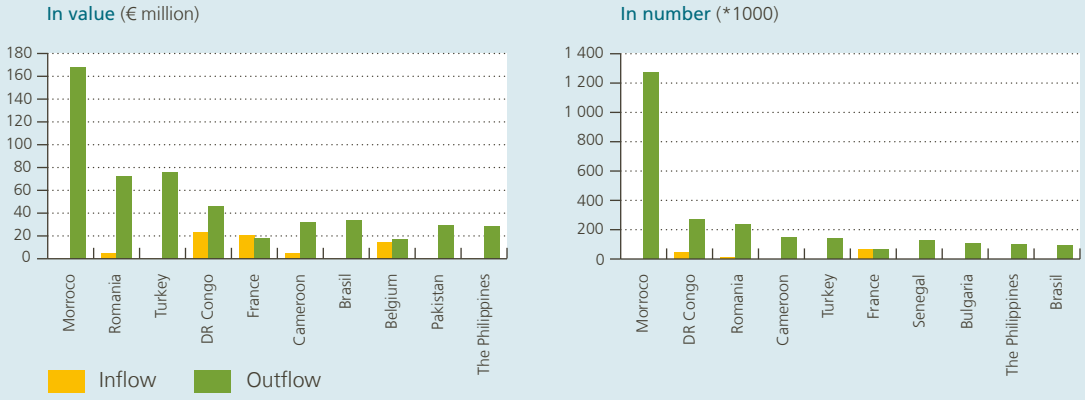


Chart 3 – Money Transfer In- and Outflow per top-10 Country Corridor

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



Source: NBB.

1 About 45 countries

Supervisory priorities in 2019

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

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

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

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

3.3 Processors of payment transactions

Changes in regulatory framework

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

Prudential & oversight approach

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

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

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

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

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

Supervisory priorities in 2019

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

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

3.4 Card payment schemes

Regulatory framework

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

1 See section 3.1 on payment systems.

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

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

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

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

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

Oversight approach

In the euro area, the sound and safe functioning of card payment schemes (CPSs) is monitored by central bank oversight. The ECB, in cooperation with the Eurosystem national central banks (NCBs), is in charge of the standard-setting process with regard to the oversight framework, as well as of the planning of assessments to be undertaken in all jurisdictions. For domestic CPSs, the compliance assessment is, as a rule, conducted by the NCB of the country where the governance authority of the CPS is established. The resulting assessment report is then peer reviewed by representatives of other Eurosystem NCBs before being submitted to the ECB and the Governing Council for publication. The monitoring of ongoing compliance also falls within the competence of the NCB from the jurisdiction where the CPS is legally established. NCBs have the discretion to apply any additional measures they deem relevant for the CPS under their oversight. The Belgian domestic CPS, Bancontact, is subject to oversight by the Bank. Therefore, the results of an assessment of its compliance with the Eurosystem CPS standards are peer reviewed at the Eurosystem level.

For international CPSs, the process is similar except that (i) the assessment work is shared among the members of the assessment group made up from representatives of the NCBs having a legitimate interest in overseeing the international CPS, the coordination of which being ensured by the lead overseer, and (ii) the peer review is *de facto* undertaken by the other members of the assessment group. This is the case for Mastercard Europe, established in Belgium, and for which the Bank ensures the role of overseer within the Eurosystem framework coordinating the assessment group.

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

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

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

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

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

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

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

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

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

Oversight priorities in 2019

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

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

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

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

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

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

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

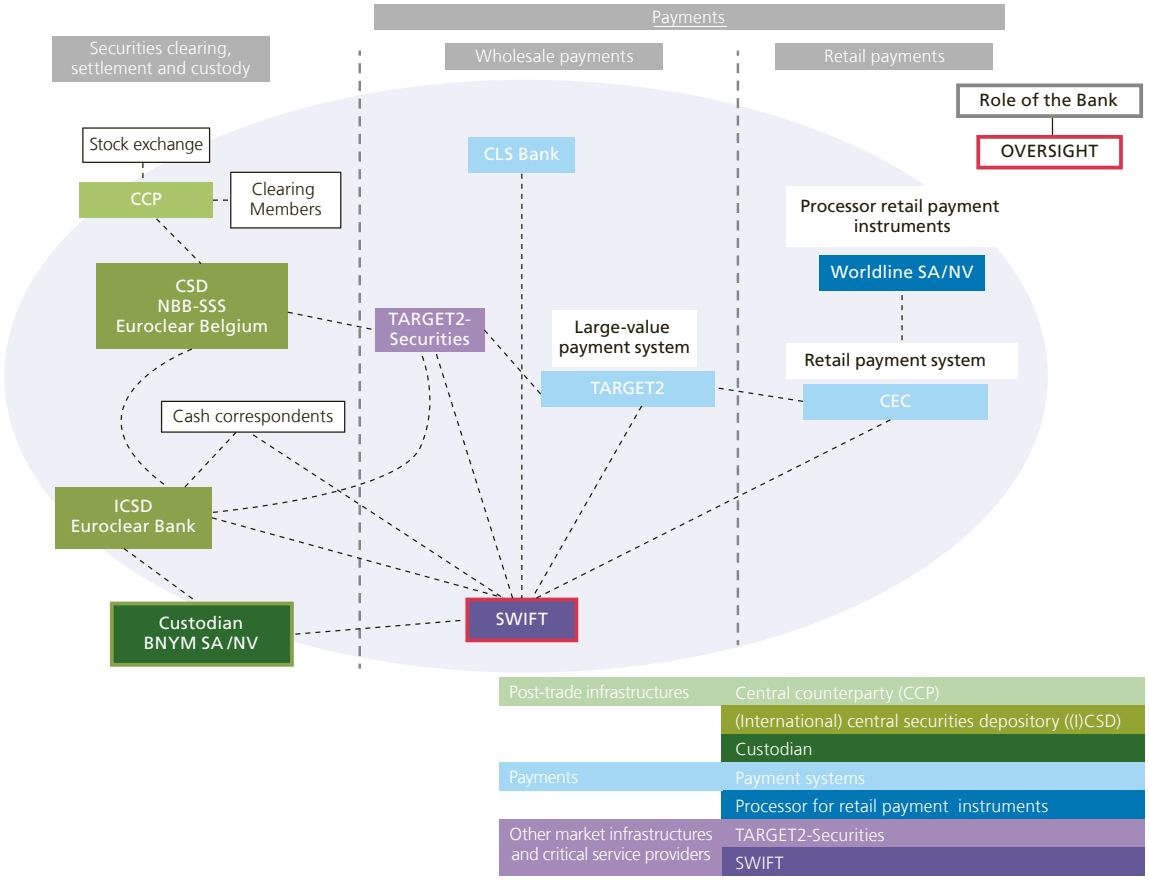
4. SWIFT

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

As a critical service provider to systemically important global correspondent banking activities and financial market infrastructures (see chart 5), SWIFT is itself of systemic importance.

Chart 5

SWIFT as a critical service provider to the financial industry and the Bank's oversight role



Oversight approach

As SWIFT's messaging activities are critical to the smooth functioning, safety and efficiency of major payment and securities settlement systems worldwide, the central banks of the G10 agreed to make SWIFT subject to cooperative central bank oversight (see Box 11).

By jointly interacting with SWIFT and formulating joint recommendations concerning it, central banks aim to improve the efficiency of both their own actions and SWIFT's actions taken in response to their recommendations. As SWIFT is incorporated in Belgium, the Bank acts as the lead overseer, in cooperation with the other G10 central banks. To complement this arrangement, the SWIFT Oversight Forum has been put in place to inform the senior overseers from CPMI member countries about SWIFT oversight conclusions. The forum also discusses oversight policy vis-à-vis SWIFT. An overview of the oversight set-up can be found in Box 12.

BOX 11

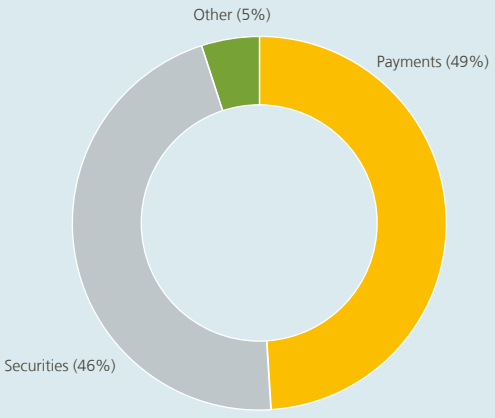
International dimension of SWIFT

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 holds shares proportional to its use of SWIFT's message transmission services. Every three years, the shares are reallocated to reflect changes in each member's use of SWIFT. The next reallocation will take place at the 2021 annual general meeting. Countries or country constituencies propose directors to the Board according to the number of shares owned by all members in the country.

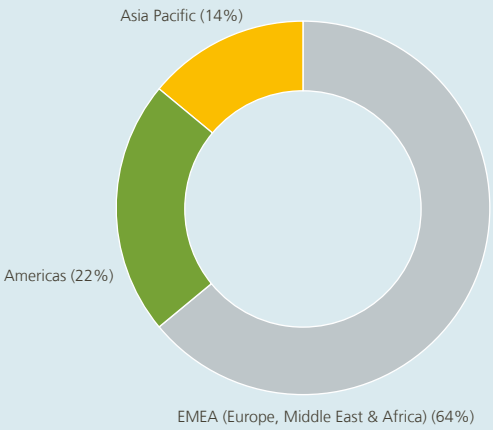
SWIFT FIN activity

(2018, based on yearly total)

Breakdown by market



Breakdown by region



Source: SWIFT.

SWIFT's customers are located in more than 200 countries and territories: there are 11 324 live users, 2 440 of whom are shareholding members. FIN is SWIFT's core messaging service for exchanging financial messages. Total FIN traffic volume in 2018 reached 7.9 billion messages (+11.3 % compared to the previous year), i.e. about 31.3 million messages per day. These messages flow between participants in stock exchanges, payment systems, correspondent banking, (I)CSDs and CCPs. In 2018, 49 % of SWIFT FIN traffic related to payments and 46 % to securities messaging (see chart below, left-hand panel), The main part of the traffic originated from EMEA members (64 %), followed by members from the Americas region (22 %) (right-hand panel).

BOX 12

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 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 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. The EG discusses the annual reporting by SWIFT's external security auditor at one of its meetings. 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 for 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 15 additional central banks (i.e. Central Bank of the Argentine Republic, Reserve Bank of Australia, Banco Central do Brazil, People's Bank of China, Hong Kong Monetary Authority, Reserve Bank of India, Bank of Indonesia, Bank of Korea, Bank of Mexico, Central Bank of Russia, Saudi Arabian Monetary Agency, Monetary Authority of Singapore, South African Reserve Bank, Banco de España and Central Bank of the Republic of Turkey)[1]. 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 platform for communication on system interdependencies related to the common use of SWIFT or for communication in the event of major contingency situations related to SWIFT.

1 Following the IMF's recommendation to consider a further broadening of the membership of the SWIFT Oversight Forum, its membership was aligned with the composition of the CPMI. Central Bank of the Argentine Republic, Banco Central do Brazil, Bank of Indonesia, Bank of Mexico and Banco de España joined the SWIFT Oversight Forum in 2019.

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

Under this framework, the overseers devoted considerable time in 2018 to monitoring SWIFT's Customer Security Programme and its Global Payments Innovation, that aims to increase the transparency and speed of cross-border payment message flows. Overseers also reviewed the expanding portfolio of SWIFT services, e.g. to detect wholesale payment fraud.

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

Customer security programme

SWIFT's Customer Security Programme aims to strengthen the security of the global financial community against cyberthreats by providing requirements for customers in terms of how they should secure their own local IT infrastructure used for connecting to SWIFT. In addition to this guidance and the establishment of a framework to foster increased transparency amongst SWIFT users on customers' adherence to the controls, the programme also focuses on making additional tools available to customers to assist them in preventing and detecting fraud in commercial relationships. Furthermore, under the programme, SWIFT takes various initiatives for sharing information, thus enabling customers to better prepare for resisting any future cyberthreats. Progress is monitored against the CPMI wholesale payment fraud prevention, detection, reaction and information sharing strategy, which is described in Box 13.

Overseers review the evolving security requirements for customers' local IT infrastructure to obtain reasonable assurance on their effectiveness in reducing the risks for SWIFT, its participants and community. An important oversight objective is to ensure that these security requirements continue to evolve in line with emerging threats, advances in cybersecurity practices and regulatory developments.

SWIFT's Customer Security Control Framework outlines the set of mandatory and advisory security controls for customers' local IT infrastructures. Mandatory security controls establish a security baseline to which all SWIFT users must adhere, whereas advisory controls describe good practices for securing local IT infrastructures.

In 2018, SWIFT presented the first revision of its Customer Security Control Framework. With this revision, SWIFT raises the security baseline by promoting three optional security best practices to mandatory requirements for the customers' local IT infrastructure. With the introduction of two additional advisory controls, SWIFT further extended its set of good practices for the customers' local IT infrastructure. Furthermore, SWIFT clarified the implementation guidelines for multiple customer security controls. The overseers ratified the proposed changes prior to publication and communicated their vision on future evolutions (including the importance of reliable fraud detection and prevention tools).

SWIFT committed to periodically improve the Customer Security Control Framework following a standardised change management strategy, which has been evaluated and accepted by the overseers. With transparent and standard adoption timeframes, SWIFT aims at improving the predictability of the process enabling participants to timely plan and budget additional measures needed to comply with the proposed updates. Change requests are captured through interaction with different stakeholders, including the overseers, SWIFT's participants and their supervisors, and cybersecurity experts. SWIFT does reserve the right to issue an emergency update to address extreme developments in the threat landscape, as strictly requested by the overseers.

All SWIFT users were required to re-assess and attest their compliance status based on each of the applicable mandatory security controls by the end of 2018. SWIFT reported an important uptake of the self-attestation process, self-attesting institutions covering more than 99 % of all FIN messages sent over the SWIFT network. The major oversight concerns in this context relate to ensuring continued customer engagement in the attestation process, participants' compliance with the evolving set of mandatory controls and the veracity of submitted self-attestations. In response to overseers' requests, SWIFT proposed an independent assurance framework covering both audit methodologies and assurance requirements.

Customers are encouraged to consult the self-attested information of their counterparties to obtain insight into their security posture and take appropriate risk mitigation measures, in order to create peer pressure to strengthen security across the ecosystem. To support this process, SWIFT introduced enhanced functionalities for the self-attestation registry (including bulk access requests and auto-grant functionality) and guidelines on including self-attestation information in counterparty risk assessments. Overseers continue to monitor the self-attestation and consultation process, as well as the level of compliance with the mandatory security controls, across different customer segments.

As of January 2019, SWIFT reserves the right to report users who have failed to timely self-attest full compliance with all mandatory security controls or who depend on non-compliant service providers (a "service bureau" or "shared infrastructure provider"), to their local supervisors. Participants must re-attest at least every twelve months and within a month after self-attestations have proven to be inaccurate (e.g. changes to the infrastructure or findings by independent assurance providers). Self-attestation information, especially information regarding non-compliance or compliance downgrades after the identification of inaccuracies by independent reviewers, could be an important input for these supervisory authorities' risk-based planning and the scoping of supervisory inspections.

The overseers requested SWIFT to report quality assurance metrics that enable an assessment of the attestation, consultation and reporting processes' effectiveness, as well as of the security gains obtained across the different participant types. Quality assurance metrics are continuously being refined and extended by the overseers to improve their monitoring activities. Based on the reported metrics, SWIFT overseers determine whether and what additional oversight demands need to be formulated.

Furthermore, overseers continue to review the adequacy of SWIFT's interface hardening and its adoption rate by SWIFT users, to examine the continuous improvement of SWIFT's Information Sharing and Analysis Centre (ISAC), to encourage reaching out to smaller users and fostering the further development of the Customer Security Intelligence team. In the context of recurring SWIFT service reviews, the overseers examined the design and implementation of new financial crime compliance messaging solutions that aim at combatting wholesale payment fraud like the Payment Control Service.

Standing oversight activities in 2018

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

In 2018, the overseers focused on the design, implementation and testing of cyberevent detection, response and recovery measures. The multi-year roadmap for further improving the cybersecurity posture of SWIFT has been reviewed, as well as assessed against the evolving threat landscape and identified technology risks. Furthermore, the overseers reviewed the scope and attack vectors used in the logical intrusion tests, as well as the implementation of the related action plans. Every year, the overseers also challenge the external security auditor' opinions and findings.

Interface products for customer connection to SWIFT are not only provided by SWIFT, but also by third parties. Rather than installing such interfaces on their premises, customers can also connect to SWIFT via a service provider (a "service bureau" or "shared infrastructure provider"). Overseers not only focused on the Customer Security Programme described earlier, but also reviewed the (cyber) risk mitigation strategies applied by SWIFT to third-party providers of interface products and shared infrastructure providers.

SWIFT's long-term strategy and how it is aligned with specific platform investments are regularly discussed with representatives of SWIFT's management and Board. Overseers typically challenge the security and strategic focus of such plans. Additionally, the overseers reviewed SWIFT's Board of Directors ISO20022 study and migration plan.

Overseers conduct regular evaluations of the effectiveness of the various lines of defence and governance structures, for daily operations, long-term strategies and specific projects. In 2018, the overseers conducted an in-depth review of the continued development of a truly integrated enterprise risk management (ERM) framework that pays due attention to other types of risk than technical or security risks (e.g. business, legal, people and third-party risk). In addition to the ERM framework's design, the overseers analysed its implementation and the interaction with SWIFT's management and Board of Directors.

When incidents take place in SWIFT's infrastructure, network or operations, the overseers investigate the sequence of events, analyse the customer impact, and review the results of the investigation. Detailed action plans that outline the activities, deadlines and responsibilities within SWIFT are requested where necessary. These action plans are frequently followed up, in order to prevent recurrence of similar incidents.

BOX 13

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

In May 2018, the Basel Committee on Payments and Market Infrastructures (CPMI) presented a strategy to encourage and help focus industry efforts towards reducing the risk of wholesale payments fraud related to compromised customer IT infrastructures [1]. Governors of the BIS Global Economy Meeting (GEM), i.e. the Governors of 30 BIS member central banks in major advanced and emerging market economies that account for approximately four fifths of the global GDP, expressed their support and commitment for operationalising the strategy within their institutions and jurisdictions.

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

1. Identify and understand the range of risks;
2. Establish endpoint requirements;
3. Promote adherence;
4. Provide and use information and tools to improve prevention and detection;
5. Respond in a timely way to potential fraud;
6. Support ongoing education, awareness and information-sharing;
7. Learn, evolve and coordinate.

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

1 https://www.bis.org/cpmi/publ/d178.htm.

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

A successful **operationalisation** of the presented strategy will depend on the active cooperation between all relevant actors, including payment system operators, participants and public stakeholders. The CPMI is committed to promoting effective and coherent operationalisation of the strategy within and across jurisdictions and systems. CPMI member central banks will act as a catalyst for the effective and coherent operationalisation of the strategy within and across jurisdictions and systems, monitor progress throughout 2018 and 2019, and where necessary take action to ensure adequate progress in the operationalisation of the strategy.

In February 2019, the CPMI organised a workshop with participants from the different stakeholders in the strategy operationalisation. Emerging practices as well as challenges faced by the different stakeholders were shared. Several multilateral groups that could assist in advancing the implementation and addressing the challenges were identified. CPMI members continue their efforts to outreach to non-CPMI central banks, regional associations and bank supervisors.

The strategy is relevant for several risk management topics covered in the CPMI-IOSCO Principles for Financial Market Infrastructures (PFMIs), Annex F of the PFMIs on oversight expectations for critical service providers and the CPMI-IOSCO guidance on cyberresilience for financial market infrastructures. It is not intended to replace or supersede them.

Oversight priorities in 2019

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

Overseers will continue to monitor relevant metrics to monitor the effectiveness of the Customer Security Programme and request the specification of additional measures where needed. Focus will be placed on the level of compliance with the security controls, the continued appropriateness of the mandatory control set in a changing environment, the effectiveness of the adherence promotion mechanisms (i.e. assurance, attestation and reporting processes) and the reach out to the different stakeholders. Special attention will be paid to SWIFT's proposals to improve the communities' confidence in the veracity of the submitted self-attestations.

These major areas of focus are complemented with continuous monitoring activities structured in line with the HLEs.

Firstly, overseers periodically assess the effectiveness of the three lines of defence (i.e. SWIFT's management, independent risk management function and internal audit function) in adequately identifying, assessing and mitigating specific risks. Due attention is paid to the further development of the ERM methodology and risk acceptance processes.

Secondly, SWIFT's business continuity management framework and disaster recovery strategies are periodically assessed against the requirements specified in the CPMI-IOSCO guidance on cyberresilience. Within this context overseers will focus on SWIFT's extreme cyberrisk scenario assessment and its progress towards the achievement of the 2-hour recovery time objective (2h RTO).

Thirdly, overseers continue assessing the risks related to strategic IT options and possible future technology renewals regarding information confidentiality, integrity and availability. Special attention will be paid to SWIFT's third party vulnerability management and incident response processes.

Fourthly, the overseers will examine the improvements to the communication processes used to inform users. The 2019 oversight priorities in this context are the communication regarding security updates (including release 7.3), the customer security programme (including communication to smaller participants, the functioning of the Customer Security Intelligence team and the distribution of actionable cyberthreat information via SWIFT's ISAC) and the customer involvement in business continuity testing.

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

Specific theme: Detecting payment fraud with artificial intelligence

Filip Caron

The cyberthreats faced by the payment system and network users have never been greater. Cyberadversaries are adopting increasingly sophisticated techniques to stealthily access users' critical assets. Forensic analyses of recent cyberincidents have uncovered highly covert malware that could bypass advanced controls like two-factor authentication. Similar threat evolutions have been reported for the retail payment market. Febelfin, the association representing the Belgian financial sector, recently reported an important increase in retail payment (e-banking) fraud as a direct result of cyberattacks. The silver linings to this evolution are an increased cybersecurity awareness and the launch of innovative artificial intelligence-based fraud detection systems.

Artificial intelligence is gaining significant traction under the impulse of converging trends. First, data is proliferating at an extraordinary rate as a direct result of increased data generation, new storage paradigms like Apache Hadoop and accessible cloud storage. Secondly, computing power has exponentially increased after decades of improvements in line with Moore's Law[1] and recent hardware innovations geared towards AI specific improvements like Spark and Googles Tensor Processing Units. Thirdly, while developing full general AI remains an objective for the far future, recent algorithmic advances have resulted in remarkable improvements in areas like image recognition.

Payment fraud detection has been identified as a promising use case for AI. Vast amounts of historical data can be analysed to identify suspicious behavioural patterns. Compared to more traditional methods, AI-based systems are expected to develop more accurate and complex criteria to determine whether a payment is likely to be fraudulent. Additionally, given the increasing demands for fast or even immediate payment processing, screening should be completed in a fraction of a second. Fraudulent transactions are frequently reported by victims to the payment system, which enables the fraud detection algorithms to identify evolving tactics.

The recognition of AI-based systems' potential to detect and ultimately prevent payment fraud has been driving the research agenda of several payment system and network operators. Examples in the wholesale and retail payment segments are provided in the box below. The aim of this article is to provide its reader with key insights into the AI concepts under research, the opportunities and challenges of applying AI in payment fraud detection as well as the relation with recent policy frameworks and strategies.

Artificial intelligence: From concept to specific techniques

Artificial intelligence (AI) focuses on simulating human-like cognitive functions, such as perceiving and correctly interpreting data, flexibly adapting and learning, as well as problem solving. Predictions and recommendations made

1 According to Gordon Moore's Law, the number of transistors on a computer chip doubles every two years. This historical trend has been observed between 1975 and 2012.

by AI-based systems are typically the result of detecting patterns in vast amounts of data, rather than executing explicit specified instructions in programme code. AI algorithms are not static but adapt and improve in response to new data.

Three objectives of data analytics are typically being distinguished, namely, in an increasing order of complexity, descriptive, predictive and prescriptive analytics. Descriptive analytics are used to describe what happens and are heavily used in the financial industry. The most promising opportunities in AI are offered by predictive analytics, that foretell what will happen in the future and prescriptive analytics, that recommend a course of actions undertaken to achieve specific objectives.

The extensive set of AI-techniques that have been proposed over the course of seven decades[1] are typically classified in three broad categories: supervised learning, non-supervised learning and reinforcement learning.

Supervised learning

A supervised learning algorithm infers a relation between the set of input variables and the output variable, based on known input-output pairs. For example, AI-based fraud detection looks at how inputs like payment value, currency and timing could be used to predict whether a payment is fraudulent or not.

The major precondition for supervised learning is that it is possible to provide a training set with known input-output pairs, which for certain payment systems and networks is available, as fraudulent payments are frequently reported thanks to incentives such as potential refunds or avoidance of further losses. The reported payments are labelled as fraudulent, while the other ones are typically considered non-fraudulent.

Once the deduced relation is considered sufficiently accurate (predetermined by the data scientist tasked with training the algorithm), the supervised learning algorithm can be applied to new data sets to determine whether they contain fraudulent payments.

More popular techniques include regression analyses, decision trees, Bayesian belief networks and simple neural networks. The Chart below provides an overview of the key constructs for the different techniques.

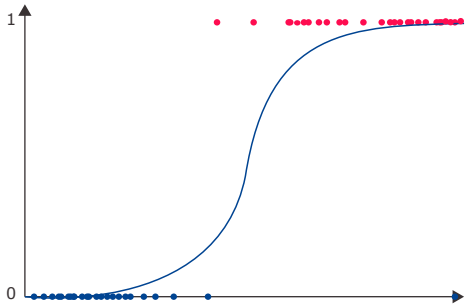
- *Linear and logistic regression analyses* are standard statistical methods that result in a mathematical expression that explicitly specifies the impact of the different input types on the output data. Regression analyses are simple to implement, but tend to be outperformed by the other techniques in this section;
- *Decision trees* provide highly interpretable classification models composed of a structure with decision nodes based on data feature values (e.g. timing) that split into branches (e.g. within versus outside normal operating hours) until a final decision output is made. In a simplistic example, the next decision node could centre on the data feature "beneficiary country", which will trigger a final decision output "fraudulent payment" if the country is on a high-country risk list;
- *Bayesian belief networks* represent the directed causal relations between events. In the context of fraudulent payments, a Bayesian belief network could include relations specifying the probability that a payment from an originator in Country X is in USD, the probability that a payment originated in Country X is fraudulent, the probability that a payment in USD is fraudulent, etc. Bayes theorem allows to calculate the probability of an event based on knowledge of other events. Bayesian belief networks allow for high computational efficiency, but require a strong understanding of typical and fraudulent payment behaviour;
- *Artificial neural networks* are algorithms that are vaguely inspired by the human brain. These networks rely on – anywhere from a few dozen to millions of – artificial neurons that process input data and influence other artificial neurons. Artificial neurons are grouped in different layers and are connected with neurons from adjacent layers. These connections between artificial neurons are weighted, with a higher weight resulting in greater influence. Artificial neural networks have a well-established history with fraud detection research. Their major downside is the high computation power needed to train and operate the neural network.

1 Artificial intelligence was founded as an academic discipline and research area in the summer of 1956 at Dartmouth College (Hanover, United States).

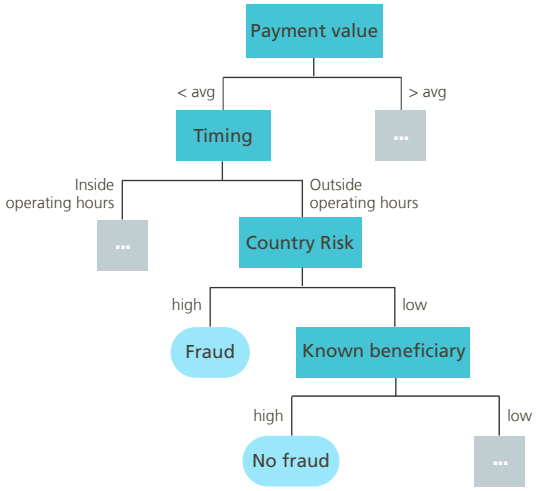
Chart 6

Key constructs in artificial intelligence (simplified examples)

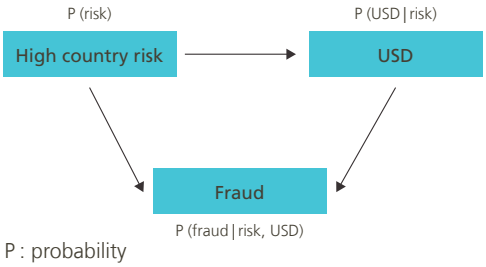
(a) Logistic regression



(b) Decision Tree

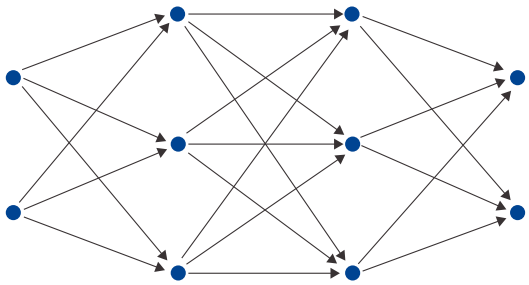


(c) Bayesian belief network



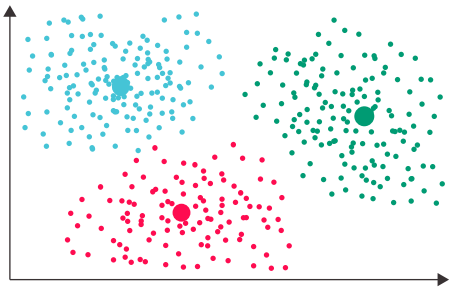
P : probability

(d) Artificial neural network



Neurons

(e) K-means clustering



Unsupervised learning

While the vast majority of AI-based fraud detection tools learn from labelled input-output pairs, several researchers reported on the use of unsupervised learning. The objective of unsupervised learning is to find patterns and a classification structure in large data sets without an explicit link between the input data and the output variable, e.g. identifying customers that exhibit similar payment behaviour (output variable, no predefined groups) based on their recent payments (input data).

A common unsupervised learning objective is clustering observations/objects, i.e. grouping data points that are highly similar to and rather different from data points in other groups. Clustering algorithms like the K-means use

iterative techniques to optimise the grouping based on predefined similarity metrics. This clustering technique has been used to group customers with similar behaviour and provide them with "standardised" payment controls to detect fraud.

But anomaly detection is probably the most interesting unsupervised learning technique objective for fraud detection. This technique monitors behaviour over time using different baselines.

- *Peer group analysis* detects users that are starting to behave in a distinctly different manner from users that were previously identified as highly similar. Increasing dissimilarity can be identified through both externally defined criteria or internal criteria which summarise previous behaviour. Peer group analysis techniques typically flag the most deviating payment behaviour as a transaction that merits closer investigation;
- *Break point analysis* aims at identifying changes in the payment behaviour of a single customer. The algorithms compare recent payment behaviour with historic data to identify material changes for the user (e.g. significant increase in the level of spending) which may not be captured with traditional rules or outlier detection techniques.

Reinforcement learning

Reinforcement learning refers to a set of AI-techniques that aim to learn how to optimise policies by trial and error. The algorithms interact with the environment and try to maximise a certain metric, e.g. optimising the return on investment of a portfolio. Reinforcement learning is typically applied in environments characterised by limited training data, vaguely specified end states or where learning about the environment is possible only through interaction. The currently limited applications of reinforcement learning have been reported in research.

Fraud detection challenges

AI-based fraud detection tools have the potential to identify potentially fraudulent payments more accurately and rapidly compared to a manual review or matching of transactions. As a result, these fraud detection tools may significantly reduce the losses (directly) related to payment fraud. However, there are some limitations.

Typical limitations of AI classification functions

As payment fraud detection is a typical classification problem, these techniques will typically be subject to issues related to the training set provided to the algorithm and to business constraints. The former typically manifest themselves when there are too little examples of fraudulent payments to learn patterns (i.e. skewed class distribution), and/or when the training set is not a good representation of all potential fraudulent behaviour, resulting in limited detection capabilities for new data sets (i.e. overfitting).

Payment processing efficiency or the time needed to initiate, clear and settle payments, is increasingly under scrutiny. While parameterisation of the algorithms is crucial in achieving maximum accuracy, (parameterisation of) the fraud detection algorithms should allow for computational efficient classifications in support of contemporary business requirements. New initiatives in the retail market like the TARGET Instant Payment Settlement (TIPS, see section 3.1) service aim at settling payments within seconds. Similarly, the Global Payments Innovation (GPI, see section 4) initiative has resulted in a significantly increased efficiency for cross-border payments, with over 50 % of the payments credited to the end beneficiaries within 30 minutes.

Ideally, payment fraud detection algorithms correctly classify all payment transactions into fraudulent and non-fraudulent categories. However, in reality there will always be false positives (legitimate payments marked as fraudulent) and false negatives (fraudulent payments marked as legitimate). False positives could result in important losses. Market research reported significant losses for retailers as a result of false declines and reputational damage for the card-issuing financial institutions.

Concept drift: fraudsters changing tactics

Supervised AI-based fraud detection techniques are extensively trained to highly accurately identify previously observed fraudulent behaviour. As the sophistication of these fraud detection techniques increases, the incentives for fraudsters to change their behaviour increase. These fraudsters have proven to be highly effective in detecting and subsequently circumventing geo-blocking and time and value constraints in the detection models.

Consequently, supervised AI-based detection techniques should be frequently updated to learn evolving trends in fraudulent behaviour. Adapting tools to changing fraudster tactics can be hard. First, retraining may demand significant computational power in case the tool is based on e.g. neural networks. Secondly, computational efficient techniques such as Bayesian belief networks require a strong prior knowledge and understanding of typical and abnormal behaviour.

Securing the fraud detection tool

Forensic cybercrime analyses of recent payment fraud-related incidents at banks have not only evidenced a significant global increase in the adversaries' level of understanding of business-oriented controls but also of the implemented security measures. Security experts reported a growing sophistication of cyberattack tactics to effectively disable and circumvent control and security measures. It is not considered unimaginable that hackers may succeed in bypassing or impacting AI-based fraud detection tools.

Network-based fraud detection services aim at mitigating the risks related to compromised environments in individual financial institutions. Payments are screened and validated in external IT environments before being cleared and settled. Credit card schemes have since long implemented network-based fraud detection techniques, and continue to further innovate in this area (e.g. MasterCard Decision Intelligence). SWIFT's Payment Control Service is an example of network-based fraud detection for wholesale payments. These examples are further explained in the box below.

Fraud detection in policy frameworks and strategies

Automated fraud detection has been recurring in recent policies, strategies and industry initiatives to reduce payment fraud.

Transaction risk analysis: risk-based exemptions for payment initiation

With the revision of the Payment Services Directive, the Commission defined a series of general security principles, including the need for a strong customer authentication (SCA). The EBA's interpretation, as described in its recent regulatory technical standards (applicable after 14 September 2019), requires verification of the customer's identity using at least two factors out of three (e.g. something you know, something you have and something you are). However, two-factor authentication might disrupt the customer experience and inhibit frictionless processing, which according to marketing research could result in significant levels of shopping-cart abandonment for online merchants.

An exemption of strong customer authentication can be obtained for small value transactions (less than € 500) if a merchant's acquiring bank has a sufficiently good fraud rate (based on the exemption threshold values) and if transaction risk analysis is implemented. This transaction risk analysis should consider geo-location, previous patterns of expenditure and all other relevant data items, making it an interesting use case for AI-algorithms. Note that even though the merchant's acquirer can claim the transaction risk analysis exemption, the issuer has the final decision and can turn down the request.

CPMI endpoint security strategy: Fraud detection in wholesale payments

Recent cyberincidents have highlighted the increasing sophistication of fraud in the wholesale payment ecosystem. Cyberattackers succeed in exploiting security weaknesses in the ecosystems endpoints (i.e. infrastructures of the connected financial institutions), resulting in both material financial risks to individual institutions and systemic risks to the ecosystem.

In response, the Committee on Payments and Market Infrastructures (CPMI) has proposed a holistic endpoint security strategy to encourage and coordinate industry initiatives. The fourth element of the strategy explicitly addresses the adoption of payment fraud detection techniques, yet another important business case for AI.

SWIFT's Customer Security Programme contains an example of the CPMI endpoint security operationalisation, the Payment Control Service being a concrete implementation of element four. The adoption of (AI-based) fraud detection algorithms is further stimulated through the advisory control (i.e. Transaction Business Control) to restrict transaction activity to validated and approved counterparties and within the expected bounds of normal business.

BOX 14

Examples of network-based fraud detection services

MasterCard Decision Intelligence (retail payment fraud detection)

MasterCard's Decision Intelligence implements data-driven algorithms to analyse and learn a specific account's spending behaviour, which after time enables the detection of abnormal behaviour. With this Decision Intelligence service, MasterCard aims at improving the accuracy of real-time approvals and reducing false declines, reducing operational expenses like chargebacks and improving customer experience.
A wide variety of account data – like customer value segmentation, risk profiling, location, merchant characteristics and time of the day – are leveraged to provide the card issuer with a predictive fraud risk score. The issuer can incorporate this predictive score in its existing fraud mitigation framework and solutions. Alternatively, the issuer could opt for MasterCard's holistic service that makes real-time decisions tailored to individual accounts.

SWIFT's Payment Control Service (wholesale payment fraud detection)

The Payment Control Service (PCS) supports SWIFT participants in detecting and preventing high fraud risk payments. As sophisticated cyberattackers would be able to circumvent payment screening controls in a compromised IT environment, the service is SWIFT-hosted with a zero footprint in the participants' IT environment.

SWIFT participants design a payment risk policy that enables real-time monitoring and alerting and blocking of sent payments. The business rules in the payment risk policy describe the expected payments behaviour, e.g. the rules cover typical characteristics like timing, thresholds, beneficiaries and currencies.

Advanced algorithms enable the identification of behavioural patterns and stimulate continuous improvement of the payment risk policy.

Annexes

Annex 1: Regulatory frameworkCSDs

FMIs	**CPMI-IOSCO Principles for Financial Market Infrastructures (PFMIs) (April 2012):** International standards for payment systems (PS), central securities depositories (CSDs), securities settlement systems (SSSs) and central counterparties (CCPs). They also incorporate additional guidance for over-the-counter (OTC) derivatives CCPs and trade repositories (TRs) http://www.bis.org/cpmi/publ/d101a.pdf
	CPMI-IOSCO Principles for Financial Market Infrastructures, Disclosure framework and assessment methodology (December 2012): Framework prescribing the form and content of the disclosures expected of FMIs, while the assessment methodology provides guidance to assessors for evaluating observance of the principles and responsibilities set forth in the PFMI. http://www.bis.org/cpmi/publ/d106.pdf
	CPMI-IOSCO Recovery of financial market infrastructures (October 2014): Guidance for FMIs and authorities on the development of comprehensive and effective recovery plans. http://www.bis.org/cpmi/publ/d121.pdf
	CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures (June 2016): Requires FMIs to instil a culture of cyber risk awareness and to demonstrate ongoing re-evaluation and improvement of their cyber resilience posture at every level within the organisation. http://www.bis.org/cpmi/publ/d146.pdf
	ECB Cyber Resilience Oversight Expectations for FMIs (CROE, December 2018): The CROE provides overseers with a framework to assess the cyber resilience of systems under their responsibility and to enable FMIs to enhance their cyber resilience. https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf
CCPs	**European Market Infrastructure Regulation (EMIR): Regulation (EU) No 648/2012 of 4 July 2012 on OTC derivatives, CCPs and TRs:** EMIR sets a clearing obligation for standardised OTC derivatives and strict CCP risk management requirements, and requires the recognition and ongoing supervision of CCPs. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012R0648&from=EN

CCPs	**CPMI-IOSCO Public quantitative disclosure standards for CCPs (February 2015):** Public quantitative disclosure standards that CCPs are expected to meet. These standards complement the Disclosure framework published by CPMI-IOSCO in December 2012. http://www.bis.org/cpmi/publ/d125.pdf
	EMIR Regulatory Technical Standards (August 2015): Regulation (EU) 2015/2205 of 6 August 2015 supplementing Regulation (EU) No. 648/2012 with regard to regulatory technical standards on the clearing obligation. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R2205&from=EN
	CPMI-IOSCO Resilience of CCPs: Further guidance on the PFMI (July 2017): Guidance providing further clarity and granularity on several key aspects of the PFMI to further improve CCP resilience. https://www.bis.org/cpmi/publ/d163.pdf
CSDs	**CSD Regulation (CSDR): Regulation (EU) No. 909/2014 of 23 July 2014 on improving securities settlement in the EU and on CSDs and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No. 236/2012:** Prudential requirements on the operation of (I)CSDs, as well as specific prudential requirements for (I)CSDs and designated credit institutions offering banking-type ancillary services. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0909&from=en
	Regulation (EU) 2017/389 of 11 November 2016 supplementing Regulation (EU) No 909/2014 as regards the parameters for the calculation of cash penalties for settlement fails and the operations of CSDs in host Member States http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0389&from=EN
	Regulation (EU) 2017/390 of 11 November 2016 supplementing Regulation (EU) No 909/2014 with regard to regulatory technical standards on certain prudential requirements for CSDs and designated credit institutions offering banking-type ancillary services https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0390&from=EN
	Regulation (EU) 2017/392 of 11 November 2016 supplementing Regulation (EU) No 909/2014 with regard to regulatory technical standards on authorisation, supervisory and operational requirements for CSDs http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0392&from=EN
Custodians	**Regulation (EU) 2017/391 of 11 November 2016 supplementing Regulation (EU) No 909/2014 with regard to regulatory technical standards further specifying the content of the reporting on internalised settlements:** Reporting obligation for settlement internalisers when settlement instructions are executed in their own books, outside securities settlement systems. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0391&from=EN

	Belgian law of 31 July 2017: Law introducing a new category of credit institutions with activities exclusively in the area of custody, bookkeeping and settlement services in financial instruments, as well as non-banking services relating thereto, in addition to receiving deposits or other repayable funds from the public and granting credit for own account where such activities are ancillary or linked to the above-mentioned services. http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=2017073111&table_name=wet / language=fr&la=F&cn=2017073111&table_name=loi
	ESMA Guidelines on Internalised Settlement Reporting under Article 9 of CSDR (March 2018) https://www.esma.europa.eu/press-news/esma-news/esma-finalises-guidelines-how-report-internalised-settlement
Payment Systems	**ECB Regulation (EU) No 795/2014 on oversight requirements for systemically important payment systems (July 2014):** Regulation, based on the CPMI-IOSCO PFMIs, covering systemically important payment systems in the eurozone, large-value and retail payment systems. https://www.ecb.europa.eu/ecb/legal/pdf/oj_jol_2014_217_r_0006_en_txt.pdf
	Revised oversight framework for retail payment systems (RPS) (February 2016): Revised framework (replacing the one from 2003) identifying RPS categories and clarifying the oversight standards applicable to each category. It also provides guidance on the organisation of oversight activities for systems of relevance to more than one central bank. https://www.ecb.europa.eu/pub/pdf/other/revisedoversightframeworkretailpaymentsystems201602.en.pdf?bc332d9a718f5336b68bb904a68d29b0
PIs & ELMIs	**EMD2 (September 2009):** Directive 2009/110/EC of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of ELMIs amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC, OJ. 10 October 2009, L. 267, 7-17. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0110&from=EN
	PSD2 (November 2015): Directive (EU) 2015/2366 of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015L2366
	Belgian Law of 11 March 2018 transposing the PSD2, Belgian Official Gazette 26 March 2018. http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=2018031107&table_name=wet / language=fr&la=F&cn=2018031107&table_name=loi
Payement Processors	**Belgian Law of 24 March 2017 on supervision of payment transactions processors,** *Belgian Official Gazette* 24 April 2017. https://www.nbb.be/doc/cp/moniteur/2017/20170424_opp_wet_loi.pdf

	Royal Decree of 8 February 2019 on the requirements for processors of retail payments instruments and card payments schemes (CPS) having established a relation with them on the due diligence that CPS must have in place when using the services of systemically relevant payment processors, the identification and management of the risks by those processors, the continuity of their services and the practical modalities of the communication in case of an incident. http://www.ejustice.just.fgov.be/eli/arrete/2019/01/25/2019030120/moniteur (FR) or http://www.ejustice.just.fgov.be/eli/besluit/2019/01/25/2019030120/staatsblad (NL)
Card Payment Schemes	**Eurosystem Oversight Framework for Card Payment Schemes (CPSs) – Standards (January 2008):** Common oversight policy to promote the reliability of CPSs operating in the euro area, public confidence in card payments and a level playing field across the euro area in a unified market. https://www.ecb.europa.eu/pub/pdf/other/oversightfwcardpaymentsss200801en.pdf
	Guide for the assessment of CPS against the oversight standards (February 2015): Assessment guide based on the Eurosystem Oversight Framework for CPSs targeting both governance authorities responsible for ensuring compliance and overseers of CPSs It has been updated by taking into account the January 2013 "Recommendations for the security of internet payments", as well as the February 2014 "Assessment guide for the security of internet payments". https://www.ecb.europa.eu/pub/pdf/other/guideassessmentcpsagainstoversightstandards201502.en.pdf?499089f7f3aab273925ef6d80767b4a5
	Regulation (EU) 2015/751 of 29 April 2015 on interchange fees for card-based payment transactions (OJ. 19 May 2015, L. 123, 1-15): This regulation contains (i) the definition of a cap for the interchange fees applicable to payment transactions by means of debit or credit cards, (ii) the separation to be put in place between payment card scheme governance activities and processing activities, (iii) measures granting more autonomy to merchants regarding the choice of payment instruments for their clients. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R0751&from=EN
	Belgian Law of 1 December 2016 transposing the EU Regulation 2015/751 of 29 April 2015, entitled "Interchange fees for card based payment transactions" (December 2016): *Belgian Official Gazette 15* December 2016, 86.578. http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=2016120112&table_name=wet / language=fr&la=F&cn=2016120112&table_name=loi
	Regulation (EU) 2018/72 of 4 October 2017 supplementing Regulation (EU) 2015/751 on interchange fees for card-based payment transactions with regard to regulatory technical standards establishing the requirements to be complied with by payment card schemes and processing entities to ensure the application of independence requirements in terms of accounting, organisation and decision-making process OJ. 18 January 2018, L. 13/1-7. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R0072&rid=3
SWIFT	**High level expectations (HLE) for the oversight of SWIFT (June 2007):** The SWIFT Cooperative Oversight Group developed a specific set of principles that apply to SWIFT. https://www.nbb.be/en/financial-oversight/oversight/critical-service-providers#oversight-of-swift-

SWIFT	**PFMIs, Annex F: Oversight expectations applicable to critical service providers (April 2012):** Expectations for an FMI's critical service providers in order to support the FMI's overall safety and efficiency. http://www.bis.org/cpmi/publ/d101a.pdf
	Assessment methodology for the oversight expectations applicable to critical service providers (December 2014): Assessment methodology and guidance for regulators, supervisors and overseers in assessing an FMI's critical service providers against the oversight expectations in Annex F. http://www.bis.org/cpmi/publ/d123.pdf

Annex 2: FMIs established in Belgium with an international dimension

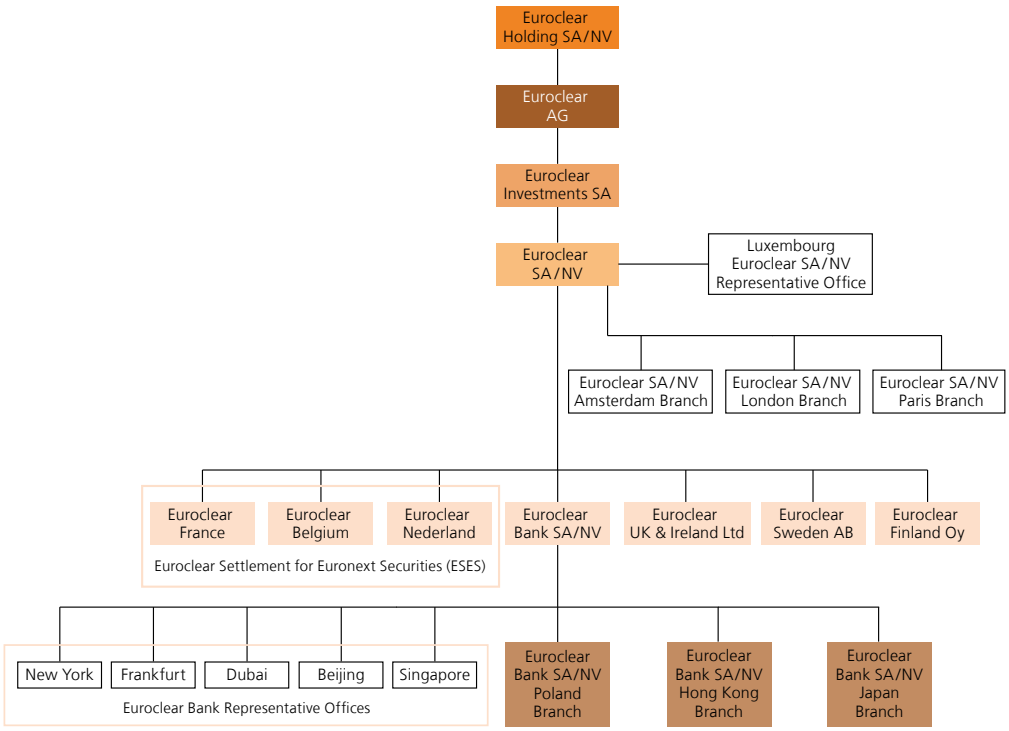
Euroclear

Euroclear Holding SA/NV, the new top financial holding of Euroclear, is incorporated under Belgian law. Euroclear Holding SA/NV owns 100 % of Euroclear AG, a new Swiss financial holding company. Euroclear Investments SA is the group's financial investment holding company, incorporated in Luxembourg.

Euroclear SA/NV (ESA), a Belgian financial holding company, is the parent company of the Euroclear Group (I)CSDs; i.e. the three ESES CSDs (Euroclear France, Euroclear Netherlands, Euroclear Belgium), Euroclear UK & Ireland Ltd, Euroclear Sweden AB, Euroclear Finland Oy and Euroclear Bank SA/NV. The latter has branches in Poland,

Euroclear Group Corporate Structure

(simplified diagram)



Source: Euroclear.

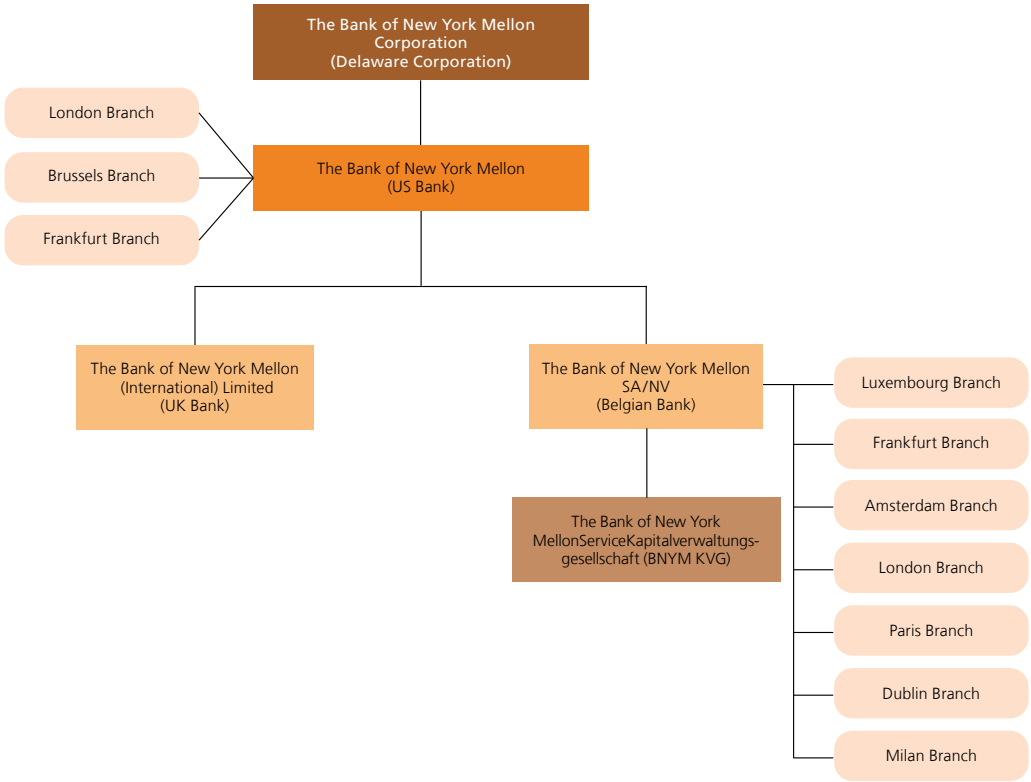
Hong Kong and Japan. Euroclear Group (I)CSDs have outsourced the IT production and development to ESA. ESA also delivers common services, such as risk management, internal audit, and legal and human resources services to the Group (I)CSDs.

Bank of New York Mellon

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

BNYM Group structure and BNYM SA/NV position

(simplified diagram)



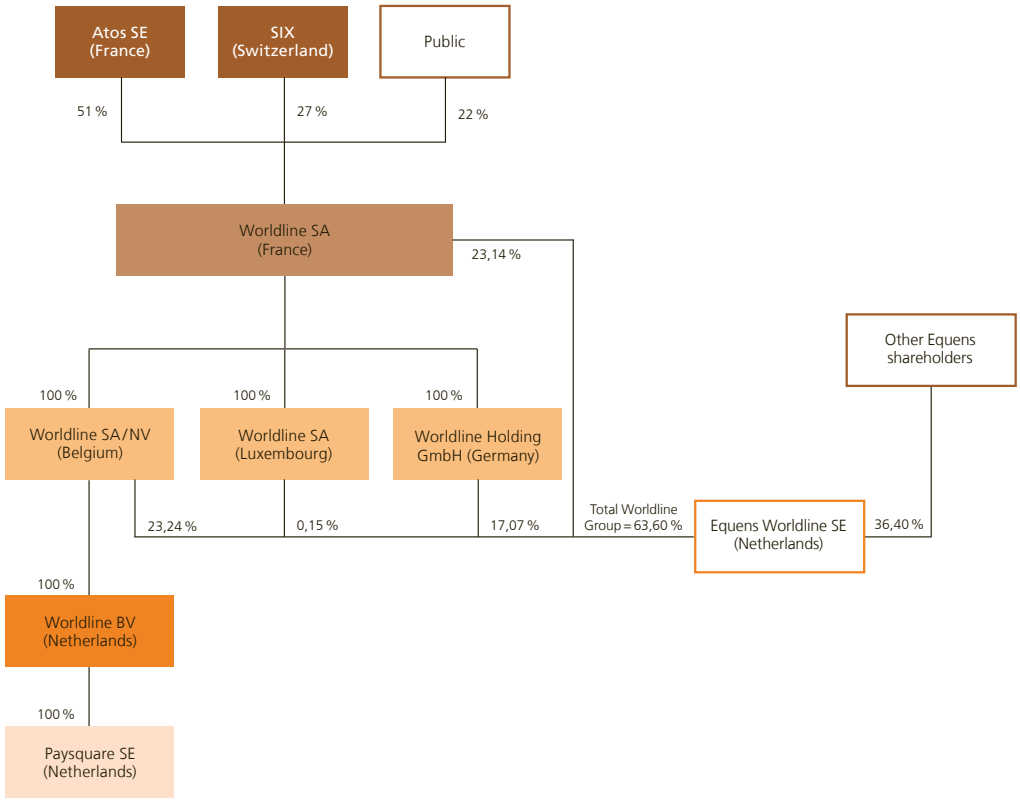
Source: NBB.

Worldline

Worldline, a division of the European IT services corporation Atos, provides electronic payment and transactional services in about 29 countries. Worldline SA is listed on Euronext Paris. In 2016, Worldline SA/NV, the Belgian entity of the group merged with the Dutch company Equens. The processing activities were carved out in a new entity called equensWorldline SE. equensWorldline SE is a partial subsidiary of several Worldline entities (Belgium, Luxembourg, France and Germany) with its historic shareholders now as minority shareholders. In 2018, Worldline acquired Six Payment Services, the payment division of the Swiss company SIX, which became shareholder (27 %) of Worldline SA.

Structure of Worldline, a division of the Atos Group

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



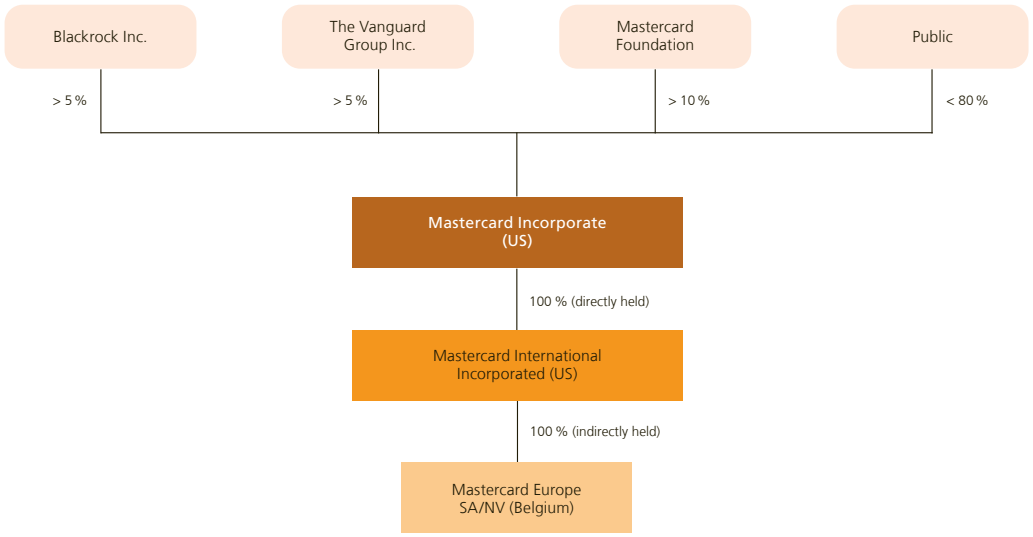
Source: NBB.

Mastercard Europe

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

Mastercard Group Structure

(simplified diagram, as of August 2017)



Source: NBB.

Annex 3: Statistics

List of tables

Table 1

Securities Clearing, Settlement and Custody

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

	2013	2014	2015	2016	2017	2018
A. Central Counterparties (CCPs) (selected)						
LCH.Clearnet Ltd (UK)						
Swapclear (including Interest Rate Swaps, Forward Rate Agreements)	362	503	489	626	807	937
Repoclear (repos)	40	41	40	37	44	49
LCH.Clearnet SA (FR)						
Credit Default Swaps (CDSClear)	0.2	0.1	0.2	0.4	0.6	0.6
Repoclear (repos)	35	33	33	34	48	50
Eurex Clearing AG (DE)						
Interest Rate Swaps	0.0	0.1	0.2	0.9	1.4	1.4
Repos	97	102	89	65	48	nav

Sources: CCP websites, NBB calculations.

Table 1 (continued)

Securities Clearing, Settlement and Custody

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

	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
B. Euroclear Bank										
Value of securities deposits (end of period)	9 832.2	10 453.8	10 766.3	10 837.2	10 834.2	11 765.3	12 393.7	12 698.4	12 834.2	13 451.5
Number of transactions (in millions)	39.3	47.7	59.4	64.2	69.5	75.2	83.3	84.1	95.4	107.0
Value of transactions	219 904.5	265 819.6	328 475.9	307 109.8	336 784.6	394 569.3	442 563.0	451 698.3	498 181.0	525 692.4
Source: Euroclear.										
C. NBB-SSS										
Value of securities deposits (end of period)	469.3	494.0	513.3	531.2	541.7	557.3	575.4	612.5	625.3	632.6
Number of transactions (in millions)	0.3	0.4	0.5	0.6	0.6	0.6	0.5	0.5	0.5	0.5
Value of transactions[1]	7 408.1	9 049.6	14 133.9	10 250.1	8 428.0	8 209.0	8 766.5	8 714.3	9 069.8	11 043.7
Source: NBB. 1 Secondary market turnover.										
D. Euroclear Belgium										
Value of securities deposits (end of period)	139.9	162.0	130.4	156.8	202.7	222.1	269.4	235.1	237.7	178.0
Number of transactions (in millions)	1.9	1.8	1.9	1.9	1.9	2.1	2.5	2.4	2.5	2.7
Value of transactions	398.5	497.7	588.0	563.6	799.8	714.8	944.6	963.8	946.0	964.1
Source: Euroclear.										
E. TARGET2-Securities										
Number of transactions (in millions)	nap	nap	nap	nap	nap	nap	7.6	36.3	125.6	145.9
Value of transactions	nap	nap	nap	nap	nap	nap	43 706.8	112 066.0	192 175.0	236 050.8
Source: ECB.										
F. BNYM SA/NV										
Value of assets held under custody (end of period)	2 480.8	2 928.9	2 667.8	2 861.9	2 905.2	3 454.0	3 216.4	3 476.5	3 608.8	2 373.1
Source: BNYM.										

Table 2

Payments

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

	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
A. TARGET2										
Value of payments	536 027.1	631 440.0	651 274.9	711 025.8	559 696.0	498 726.5	508 982.3	485 811.8	432 780.7	432 508.1
of which: TARGET2-BE	20 835.2	20 199.7	22 163.2	18 712.6	16 177.3	16 247.9	15 627.4	16 957.9	19 732.4	22 594.7
Number of payments (in millions)	87.8	87.2	89.0	89.6	91.3	87.8	88.6	89.0	89.3	88.4
of which: TARGET2-BE	2.1	2.4	2.6	2.5	2.3	2.5	2.3	2.2	2.3	2.3
Source: ECB Payment Statistics. RTGS related payments, excluding TARGET2 transactions on Dedicated Cash Accounts. Last year's figures from https://www.ecb.europa.eu/stats/payment_statistics/large_value_payment_systems/html/index.en.html.										
B. CLS Bank										
Value of payments (in € trillion)	607 499.9	781 426.9	893 590.4	878 469.0	897 145.6	1 042 062.3	1 118 933.9	1 162 359.8	1 193 728.3	1 282 149.3
of which: EUR payments	131 665.9	161 791.1	182 482.0	185 881.3	182 305.8	191 170.5	208 555.8	204 370.7	219 924.6	241 067.1
Number of payments (in millions)	150.1	198.1	206.9	176.6	205.0	204.7	219.1	209.5	198.5	226.6
of which: EUR payments	31.8	42.2	45.5	37.4	36.9	34.4	40.9	34.3	34.0	39.1
Source: CLS.										
C. Centre for Exchange and Clearing (CEC)										
Value of payments	804.9	846.9	886.7	909.1	911.6	870.7	883.4	920.6	941.8	1 122.9
Number of payments (in millions)	1 122.9	1 170.2	1 224.9	1 295.1	1 365.6	1 272.2	1 402.2	1 387.1	1 312.0	1 456.7
Source: NBB.										

Table 2 (continued 1)

Payments

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

	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
D. Payment Institutions (PIs) – Electronic Money Institutions (ELMIs)										
PIs										
Belgian PIs	0	1	9	9	11	15	17	21	24	22
Foreign PIs with Belgian branch	0	0	0	2	2	3	3	3	2	3
Passport notifications for cross-border services										
Belgian PIs towards other EEA countries	0	11	19	19	26	41	65	162	218	248
Foreign EEA PIs towards Belgium	22	47	104	133	184	262	273	379	421	435
ELMIs										
Belgian ELMIs	4	6	6	6	10	10	10	8	8	7
Foreign ELMIs with Belgian branch	0	0	0	0	0	1	1	1	1	2
Passport notifications for cross-border services										
Belgian ELMIs towards other EEA countries	12	15	18	19	43	45	69	70	72	72
Foreign EEA ELMIs towards Belgium	7	8	14	28	40	54	53	102	156	188
Institutions offering services within a limited network (new under PSD2)	nav	nav	nav	nav	nav	nav	nav	nav	nav	1
Transactions by Belgian PIs and ELMIs (in millions)										
Number of transactions (yearly total)	nav	nav	nav	nav	1 665	1 874	1 968	2 155	2 006	2 044
Value of transactions in euro (yearly total)	nav	nav	nav	nav	105 989	133 513	136 567	137 144	124 388	124 485
Average outstanding E-Money of Belgian ELMIs	nav	nav	nav	nav	15.2	21.8	35.8	45.5	73.9	116.6
Source: NBB.										
E. Processors of payment transactions										
Worldline SA/NV										
Number of transactions (yearly total, in millions)	1 230.1	1 295.5	1 387.6	1 473.7	1 553.9	1 665.8	1 800.0	1 960.0	2 150.0	nav
Source: Worldline.										

Table 2 (continued 2)

Payments

	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
F. Card transactions										
Number of cards issued by resident payment service providers – Cards with a cash function										
Number of cards (in thousands of numbers, end of period)			20 005.19	20 647.08	20 041.34	21 396.54	21 870.76	22 593.13	22 362.50	nav
Number of cards per capita (end of period)			1.82	1.87	1.80	1.92	1.95	2.00	2.00	nav
POS transactions at terminals provided by resident PSPs										
Number of payment transactions per card – With cards issued by resident PSPs (yearly total)			52.41	54.2	60.2	58.4	61.8	67.4	75.2	nav
Value of payment transactions per card – With cards issued by resident PSPs (yearly total, in €)			2 752.94	2 838.92	3 091.49	2 906.16	2 948.40	3 094.6	3 343.8	nav
Transactions per capita										
Number of card payments – With cards isssued by resident PSPs [1] (yearly total)			105.15	111.0	120.0	135.2	138.9	151.0	166.7	nav
Value of card payments – With cards issued by resident PSPs [1] (yearly total, in € thousands)			5.77	6.1	6.4	6.6	6.9	7.1	7.7	nav

Source: ECB Payment Statistics.

1 Except cards with an e-money function only.

G. Card schemes										
Bancontact – Number of transactions (yearly total, in millions)			1 076.4	1 136.4	1 180.4	1 241.8	1 306.7	1 389.5	1 441.6	1 480.2
of which:										
Retail payments			973.4	1 028.9	1 068.4	1 125.9	1 190.9	1 272.8	1 325.2	1 336.0
ATM			103.0	107.5	111.9	115.9	115.9	116.8	116.3	114.2

Source: Bancontact.

Table 3

SWIFT

(yearly total, in millions)

	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
Number of messages	3 760.3	4 031.9	4 433.9	4 589.1	5 065.7	5 612.7	6 106.6	6 525.8	7 076.5	7 873.6
of which:										
Payment messages	1 933.9	2 041.4	2 157.5	2 314.4	2 524.5	2 737.2	2 930.2	3 139.3	3 485.2	3 840.0
Securities messages	1 583.5	1 723.2	1 945.9	1 975.3	2 215.6	2 545.2	2 829.1	3 019.1	3 232.3	3 635.5
Other messages	242.9	267.3	330.5	299.4	325.6	330.3	347.3	367.3	359.0	398.1

Source: SWIFT.

List of abbreviations

AISP	Account information service provider
ASPSP	Account servicing payment service provider
BNYM	Bank of New York Mellon
CCP	Central counterparty
CEC	Centre for Exchange and Clearing
CLS	Continuous Linked Settlement
CPMI	Committee on Payments and Market Infrastructures
CSDR	CSD Regulation
CSD	Central Securities Depository
DvP	Delivery versus payment
EBA	European Banking Authority
ECB	European Central Bank
EEA	European Economic Area
ELMI	Electronic money institution
EMD	Electronic Money Directive
EMEA	Europe, Middle East and Africa
EMIR	European Market Infrastructure Regulation
EPC	European Payments Council
ESA	Euroclear SA/NV
ESCB	European System of Central Banks
ESES	Euroclear Settlement of Euronext-zone Securities
ESMA	European Securities and Markets Authority
FMI	Financial market infrastructure
FSB	Financial Stability Board
FSMA	Financial Services and Markets Authority
G-SiFI	Global systemically important financial institution
ICSD	International central securities depository
IFR	Regulation on interchange fees for card-based payment transactions
IOSCO	International Organisation of Securities Commissions
ISAC	Information sharing and analysis centre

LSE	London Stock Exchange
LSI	Less significant institution
LVPS	Large-value payment system
MCE	MasterCard Europe
MoU	Memorandum of Understanding
NCA	National competent authority
NCB	National central bank
ORPS	Other retail payment system
O-SII	Other systemically important institution
OTC	Over the counter
PFMIs	CPMI-IOSCO Principles for FMIs
PI	Payment institution
PISP	Payment initiation service provider
POS	Point of sale
PSD	Payment Services Directive
PSP	Payment Service Provider
PvP	Payment versus payment
RPS	Retail payment system
SCT Inst	SEPA instant credit transfer
SEPA	Single European Payments Area
SI	Systemically-relevant credit institution
SIPS	Systemically important payment system
SSM	Single supervisory mechanism
SSS	Securities settlement system
SWIFT	Society for Worldwide Interbank Financial Telecommunication
T2	TARGET2
T2S	TARGET2-Securities

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

Publisher

Tim Hermans
Executive Director

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

Contact for the publication

Johan Pissens
Deputy Director
Surveillance of financial market infrastructures, payment services and cyber risks

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

Cover and layout: NBB AG – Prepress & Image

Published in June 2019

Printed on FSC paper