

Financial Market Infrastructures and Payment Services Report 2020



Financial Market Infrastructures and Payment Services Report 2020

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, C. Cabaret, F. Caron, C. Collaert, D. De Beuckeleer, P. Gourdin, D. Gui, I. Meau, L. Ohn,
V. Olecrano, S. Siedlecki, C. Stas, R. Temmerman, M. Van Acoleyen, S. Van Cauwenberge, I. Vansieleghem,
J. Vermeulen

© National Bank of Belgium

All rights reserved.
Reproduction of all or part of this publication for educational and
non-commercial purposes is permitted provided that the source
is acknowledged.

Contents

Executive summary	7
1. The Bank's role in oversight and prudential supervision of financial market infrastructures, custodians, payment service providers and critical service providers	9
1.1 Critical nodes in the functioning of financial markets and payment services	9
1.2 FMIs, custodians, payment service providers and critical service providers subject to oversight and prudential supervision by the Bank	14
2. Securities clearing, settlement and custody	19
2.1 CCPs	20
2.2 (I)CSDs	23
2.3 Custodians	34
3. Payments	39
3.1 Payment systems	42
3.2 Payment Institutions and Electronic Money Institutions	43
3.3 Processors of payment transactions	51
3.4 Card payment schemes	51
4. SWIFT	53
4.1 Oversight approach	54
4.2 Covered oversight topics in 2019	59
4.3 Oversight priorities in 2020	61
5. Thematic article : Emerging practices for pandemic resilience	65
Annexes	71
1. Regulatory framework	73
2. FMIs established in Belgium with an international dimension	79
3. Statistics	83
4. List of abbreviations	91

Executive summary

Belgium hosts a number of significant financial market infrastructures (FMIs), custodians, payment service providers, such as payment institutions and electronic money institutions, as well as critical service providers and card payment processors, some of which also have a systemic relevance internationally. This Financial Market Infrastructures and Payment Services Report aims to provide a comprehensive overview of the National Bank of Belgium's oversight and supervision of these systems and institutions headquartered in, or relevant for, Belgium.

Over the last few years, several major international regulatory initiatives have been launched in the area of FMIs and payment services. In Europe, this has led to new pieces of legislation like the Payment Services Directive 2 (PSD2) and the Central Securities Depository Regulation (CSDR). The approach taken here was creating specific regulatory categories of institutions that could provide certain payment services or CSD services, setting up regulatory requirements, including the need to get licences, and the setting up of a supervisory regime.

After the phases of standard-setting and providing regulatory guidance and detailed regulatory technical standards, the regulatory emphasis has now gradually evolved to licensing institutions under these new regulatory frameworks: in 2019, under the CSDR, the NBB granted licences to two central securities depositories, and, under the PSD2, to two electronic money institutions, seven payment institutions and one payment institution providing account information services.

PSD2 and retail payments

The entry into force of PSD2, and in particular the “open banking” provisions, led to requests for licences by new types of institutions: payment initiation service providers and account information service providers. The year 2019 saw a significant increase in the number of authorised payment institutions and electronic money institutions in Belgium. This was not only due to the entry into force of PSD2 but also to UK-based payment institutions that have set up a legal entity in Belgium in anticipation of the UK's departure from the EU.

The PSD2 open banking provisions require account-servicing payment service providers (mainly banks) to open their online payment account infrastructure for access by licensed institutions (such as other banks and payment institutions). This enables these institutions to provide to their own customers payment initiation services and account information services, thereby boosting competition in the payment services market. Access to this payment accounts infrastructure is regulated with strict security requirements which must be respected by all the payment service providers concerned. The compulsory opening up of payment accounts was brought about mainly by means of a dedicated interface developed by the banks.

Another major development for underpinning innovative payment services and instruments relates to so-called faster payments. As of 4 March 2019, the Centre for Exchange and Clearing (CEC) has been able to process instant payments (retail payments that are executed within 5 seconds, even outside regular business hours and at weekends). The volumes processed are growing regularly and peaked at more than 400 000 operations per day by the end of 2019.

Cyber risks

Given the nature of their activity, operational risk is of paramount importance for FMIs and payment services providers. The NBB's oversight and prudential activities have an ongoing focus on operational resilience, including business continuity requirements. A particular area for attention is that of cyber risks. Cyber crime has been on a continuous rise over the last few years, with a significant focus on the financial sector, in particular on FMIs and payment services providers.

The NBB's oversight and supervision takes into account the importance of end-to-end security in the transaction chain, in line with the Committee on Payments and Market Infrastructures (CPMI) 2018 Strategy for reducing the risk of wholesale payment fraud related to end-point security. The SWIFT Customer Security Control Framework (CSCF), which aims to strengthen the security of the global financial community against cyber threats by providing requirements for users in terms of how they should secure their own local IT infrastructure used for connecting to SWIFT, has been analysed by overseers on the effectiveness of the implementation and reporting processes. This follow-up has included monitoring progress of adherence to and raising awareness about cyber controls under the CSCF and assisting in promotion of the framework with bank supervisors. The Bank also monitored implementation under the CSCF by institutions under its oversight work in 2019.

Internationally active FMIs and critical service providers

Belgium is home to a number of internationally active FMIs and critical service providers, such as SWIFT and Euroclear, which are also systemically relevant in other jurisdictions. In these cases, the Bank's oversight and supervision is organised through international cooperative arrangements with other central banks and/or regulators, in line with Responsibility E of the CPMI-IOSCO Principles for FMIs. Over the years, the Bank has set up processes to periodically review, and where necessary adapt, these arrangements, in order to ensure their efficiency and effectiveness, and to align them with the new regulatory frameworks, such as the CSDR.

Resilience during the COVID-19 crisis

This Report also gives an initial picture of FMIs', payment service providers' and critical service providers' resilience during the COVID-19 crisis. Most of them were well prepared to deal with extreme scenarios and could thus smoothly switch to BCP arrangements such as wide-scale home working for staff.

Pandemic recovery plans that enable FMIs to continue providing robust platforms and operations consider challenges that deviate from those encountered in more stereotypical business continuity scenarios. Unlike incidents caused by natural disasters, infrastructure failures or cyber attacks, the pandemic scenario needs to consider prolonged and potentially recurring periods of widespread operational stress. A pandemic is not a one-off incident impacting a specific location. Based on experience and the lessons learned so far, the thematic article in section 5 presents an initial overview of emerging practices for pandemic resilience.

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

To provide more insight into 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 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 crises. At the same time, they are interlinked with other financial market infrastructures (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 2019 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). The final investor uses a custodian bank, which 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 this Report.

FMI 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)CSDs² 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 markets worldwide, it is considered a global custodian.

Payments

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

Payment systems encompass 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 by means of credit transfers and direct debits. In Belgium, most interbank 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.

The role of PIs and ELMIs in the retail payments area is multiple and growing. PIs and ELMIs have since long been active in the card payment business, issuing payment cards to the user and/or acquire the funds for the payment on behalf of the merchant. The second Payment Services Directive (PSD2) will further strengthen the role of non-banks in the market since they are now allowed (under certain conditions) to make use of the banking industry's accounting ledger for accessing and consulting payment service users' accounts online.

Card payments remain the most widely used payment instrument in Belgium and 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

¹ 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.

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 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 Mastercard group, which owns the international (credit) card payment scheme, and is established in Belgium. For Bancontact, a scheme switch is in place, but one processor provides the underlying network and services for the majority of card payments, namely equensWorldline SE. For Maestro, the processing network is provided directly by Mastercard. After the processing of card payments, transactions are sent to the CEC for clearing and settlement. Pls have also a major role in providing money transfer/remittance services (fund transfers) allowing retail customers to transfer funds from Belgium to a third party in different locations around the world and vice versa.

CLS, a 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 eliminates FX settlement risk when – due to time zone differences – one party transfers the currency it sold but does not receive the currency it bought from its counterparty.

Other infrastructures and service providers

TARGET2-Securities (T2S) is the common settlement platform for European CSDs. Although SWIFT, which provides messaging services, 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

For most of the institutions mentioned in the following graph, the growth in number and value of transactions continued in 2019.

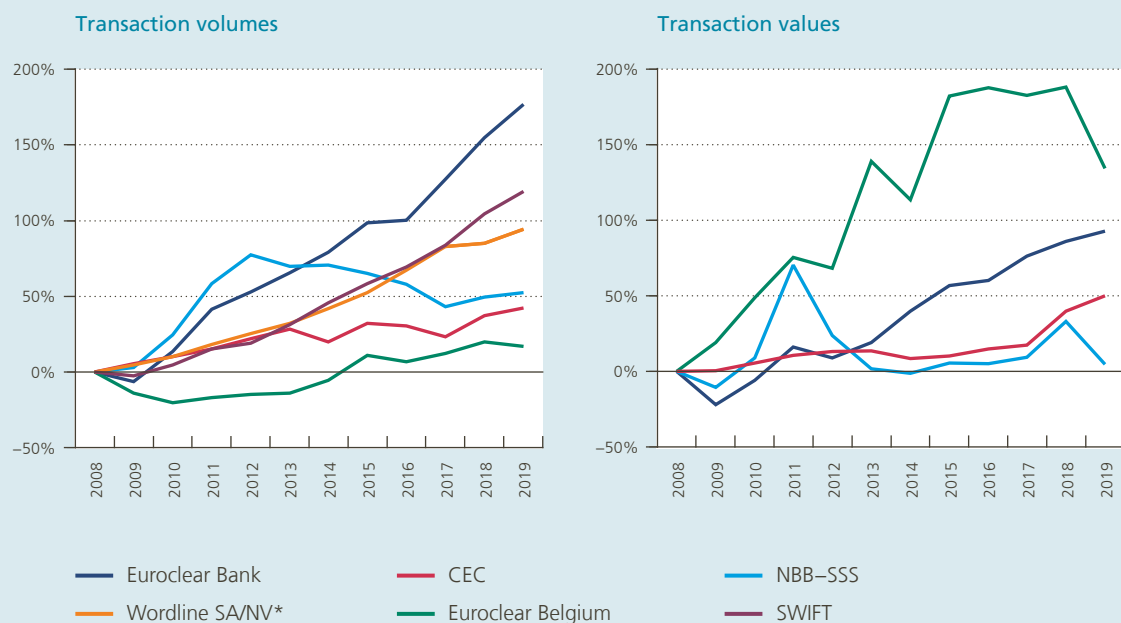
The underlying factors that could explain the evolution in FMIs' and service providers' business activities can be diverse (e.g. market volatility in wholesale markets, digitalisation of retail payments). Some of them have expanded their activity considerably since reference year 2008. In terms of transaction volumes, this is notably the case for Euroclear Bank (+177%) and SWIFT (+119%). In value terms, highest growth rates are recorded for Euroclear Belgium (+134%)¹ and Euroclear Bank (+93%). 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 the impact of the sovereign debt crisis in 2011).

¹ Euroclear Belgium settles mainly equities that are expressed in terms of market value.



Trends in transactions processed by selected FMIs and service providers

(in %, reference year 2008 as index 0)



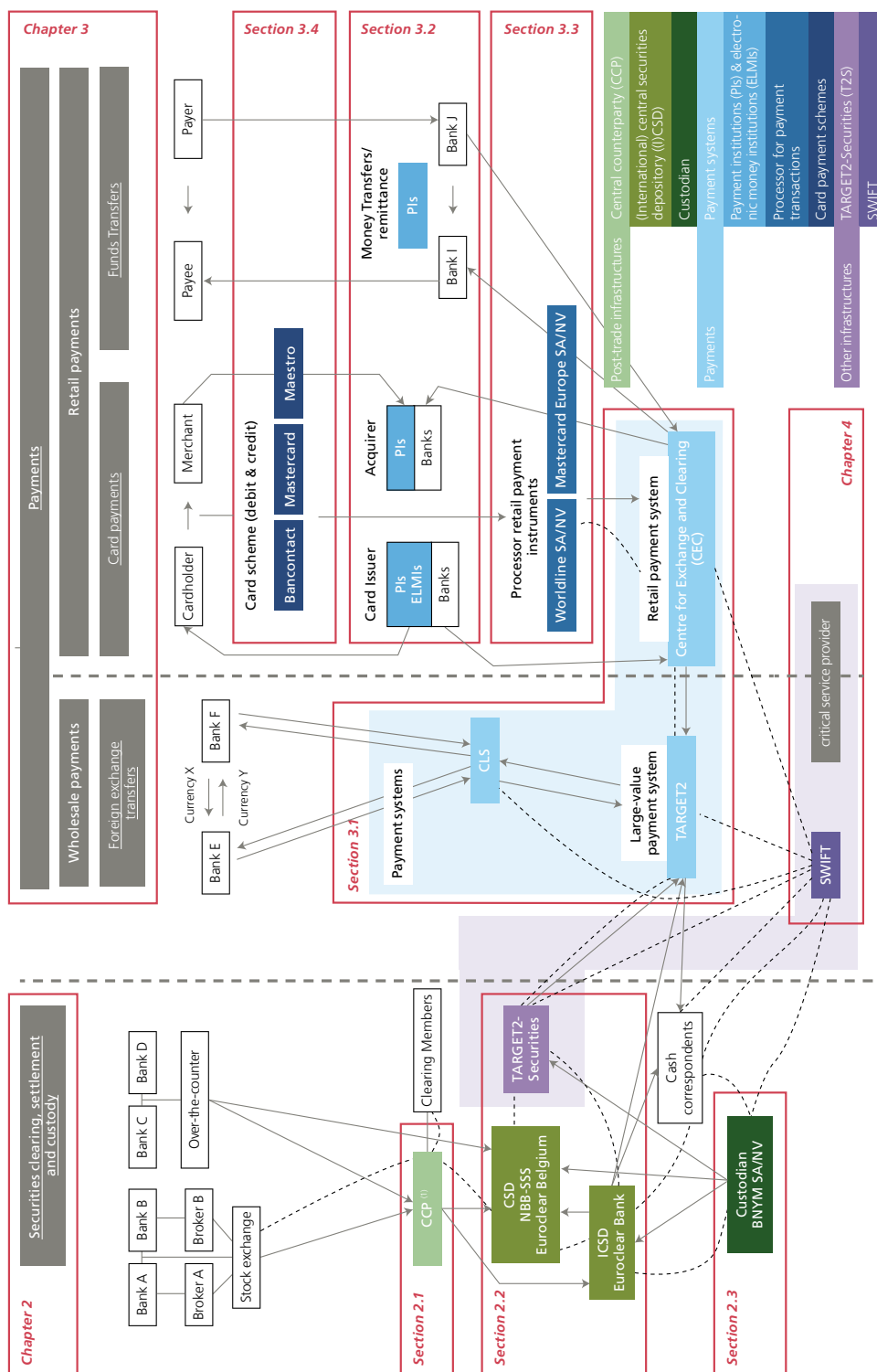
* Since 2017, as a consequence of the transfer of some processing activities to equensWorldline SE, volumes reported in this chart only refer to acquiring activities of Worldline SA/NV

Source: NBB calculations.

In general, the systemic importance of these FMIs and service providers continues to grow. An unexpected disruption of their services could have a significant impact across different types of stakeholders (including the public in general). Operational resilience of FMIs and 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 the event of cyber attacks.

Chart 1

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



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

The Bank has responsibilities in both oversight and prudential supervision of FMIs, custodians, PSPs, such as Pls and ELMIs and critical service providers.

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

Central banks have always had a close interest in the safety and efficiency of payment, clearing and settlement systems. One of the principal functions of central banks is to be the guardian of public confidence in money, and this confidence depends crucially on the ability of economic agents to transmit money and financial instruments smoothly and securely through payment, clearing and settlement systems. These systems must therefore be strong and reliable, available even when the markets around them are in crisis and never themselves be the source of such crisis. The central bank's oversight of FMIs 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 Law¹ and focuses on systems established in, or relevant for Belgium. Although SWIFT is neither a payment, clearing nor 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, in which the Bank has the role of lead overseer.

The Bank is also prudential supervisory authority for individual financial institutions, as well as custodians and PSPs like Pls and ELMIs. While significant credit institutions, such as The Bank of New York Mellon SA/NV (BNYM SA/NV), are directly supervised by the single supervisory mechanism (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). Worldline SA/NV is also subject to both prudential supervision (as PI) and oversight (as processor of retail payment instruments). 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 CPMI-IOSCO Principles for FMIs (PFMIs)), the prudential supervision focuses on the financial soundness of the operator (by assessing compliance with prudential regulations). As a result, oversight and prudential supervision typically cover different topics or different perspectives. 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 focuses on cover the functioning of the system and how its organisation and operation minimises or avoids risks not only for itself but – just as importantly – for its participants. Examples include settlement finality rules reducing risks associated with 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.

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 rely on different frameworks. For oversight, the PFMI cover payment systems, securities settlement systems, CSDs, CCPs and trade repositories, as well as critical service providers (Annex F of the PFMI report). 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

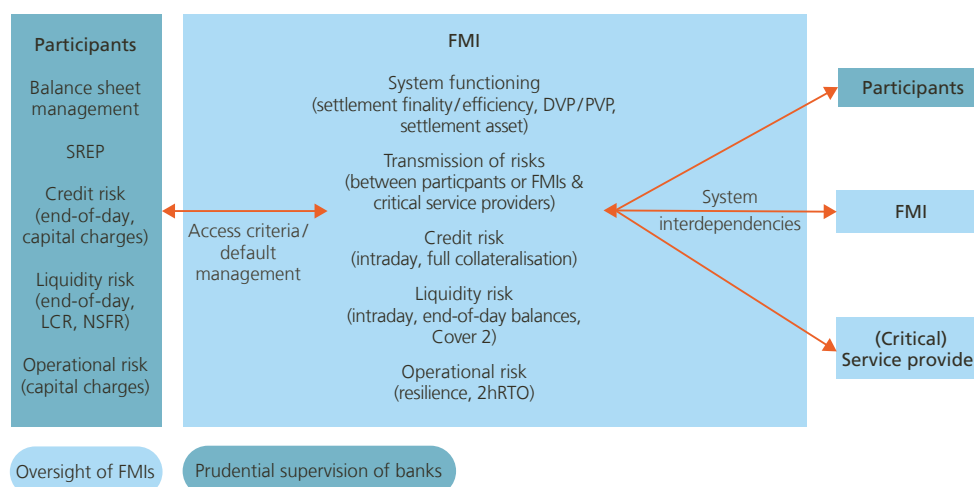
Table 1

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 SIPS, EMIR and CSDR)	Directives/Regulation ("hard law" approach)
Selected examples of attention points	<ul style="list-style-type: none"> ■ 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) 	<ul style="list-style-type: none"> ■ 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

Chart 2

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



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 retail payment instruments. Also, the EU transposed the oversight framework for CCPs and CSDs (i.e. PFMI) 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.

Some FMIs or PSPs, such as Euroclear Bank or Worldline, are subject to both oversight and prudential supervision. In order to pool expertise, reinforce the synergies and align approaches 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 for these categories of institutions.

Table 2 below provides an overview of the systems and institutions supervised and/or overseen by the Bank for these categories of institutions. 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 authorities². These may involve multilateral cooperative arrangements, in which the Bank acts as lead overseer (Euroclear, SWIFT). The Bank also takes part in a number of international cooperative arrangements (CCPs, BNYM, 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.

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 it does not have any formal cooperation but which may be interested in understanding the applicable framework, the regulatory approach and the main supervisory priorities.

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

(January 2020)

	International supervisory college / cooperative oversight arrangement		NBB solo authority
	NBB lead authority	NBB takes part, other authority is lead	
Prudential supervision		<u>Custodian</u> Bank of New York Mellon SA/NV	<u>Payment Service Providers (PSPs)</u> <u>Payment Institutions (Pis)</u> <u>Electronic Money Institutions (ELMIs)</u>
Prudential supervision and oversight	<u>CSD</u> Euroclear Belgium (ESES) <u>ICSD</u> Euroclear Bank SA/NV <u>Institution providing support to a CSD</u> Euroclear SA/NV (ESA)	<u>CCP</u> LCH Ltd (UK), ICE Clear Europe (UK) LCH SA (FR), Eurex Clearing AG (DE), EuroCCP (NL), Keler CCP (HU), CC&G (IT)	<u>Processor for retail instruments</u> Worldline SA/NV
Oversight	<u>Critical service provider</u> SWIFT	Market infrastructure TARGET2-Securities (T2S) ¹	<u>CSD</u> NBB-SSS
		<u>Payment system</u> TARGET2 (T2) ¹ CLS	<u>Card payment schemes</u> Bancontact ¹ Mastercard Europe ¹ Maestro ¹
			<u>Processor for retail instruments</u> Mastercard Europe
			<u>Payment system</u> Centre for Exchange and Clearing (CEC) ¹
Post-trade infrastructures	Securities clearing	Payments	Payment systems
	Securities settlement		Payment institutions and electronic money institutions
	Custody		Processors for retail payment instruments
			Card payment schemes
Other infrastructures	T2S		
	SWIFT		

Source: NBB.

¹ Peer review in Eurosystem/ESCB.

2. Securities clearing, settlement and custody

FMI 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, the systemic relevance of which has grown after EMIR 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 EMIR, the Bank takes part 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 SSM. However, being an LSI, 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 (Capital Requirements Directive/Capital Requirements Regulation, etc.) do not always adequately cover the specific operational and financial risks involved. Other internationally agreed standards for CCPs and (I)CSDs are more suited for covering such risks (i.e. PFMI). 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 by Belgian law as the sole competent supervisory authority¹ for Euroclear Bank and Euroclear Belgium, and, as overseer, is also considered as the relevant authority in the CSDR. The NBB-SSS, which is subject to oversight only, 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.

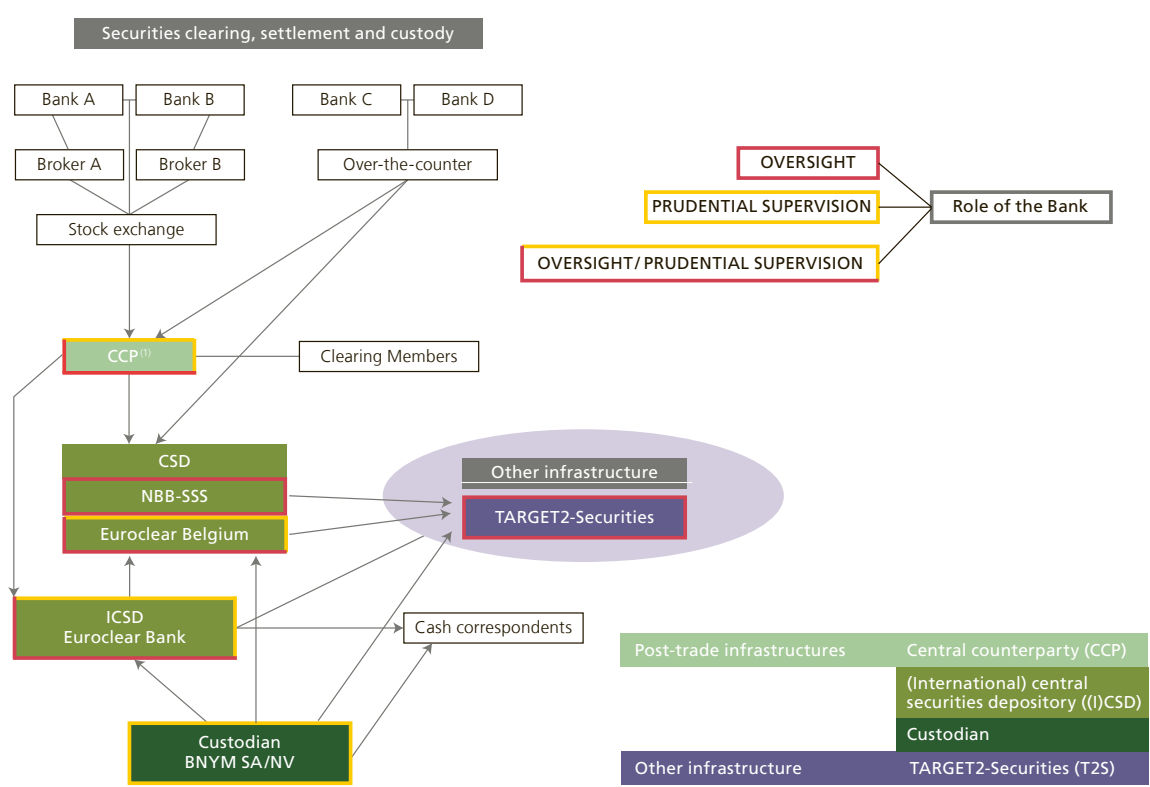
Daily settlement operations in Euroclear Belgium and NBB-SSS are outsourced to TARGET2-Securities (T2S), as in the case of other CSDs in Europe. T2S is not a CSD, but as it provides settlement services to many euro area and some non-euro area CSDs, it is essential that it enables member CSDs to comply with the regulations applicable to them. T2S is overseen by the Eurosystem. Furthermore, in line with PFMI Responsibility E (Cooperation with other authorities), the Eurosystem has set up the T2S Cooperative Arrangement, coordinated by the ECB and ESMA, to ensure that all authorities with a legitimate interest in the smooth functioning of T2S are involved, including the overseers, supervisors, and market authorities of

¹ For the aspects mentioned in the footnote on page [25], the Bank consults the FSMA, which retains its competence as market authority.

CSDs that have signed the T2S Framework Agreement. Oversight assessments of T2S cover 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 and are conducted against an applicable sub-set of PFMLs. The Bank is involved in the Eurosystem oversight of T2S and the T2S Cooperative Arrangement.

Finally, section 2.3 covers institutions whose single business line is the provision of custodian 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

As there are no CCPs located in Belgium, some foreign CCPs are also used by Belgian financial institutions for clearing and use Belgian FMIs for settlement (see chart 3), and therefore the Bank closely follows up developments regarding CCPs. The main changes in the regulatory framework are summarised below.

The Financial Stability Board's 2015 workplan¹ to strengthen CCP resilience and recovery, and ultimately CCP resolution has been implemented with the exception of a last piece related to resolution.

To complete the 2017 FSB guidance on CCP Resolution², the FSB consulted the market at the end of 2018 on two further aspects, the availability of financial resources for CCP resolution and the treatment of CCP equity in resolution. The consultation together with input from CCP crisis management groups, i.e. the groups of authorities that will cooperate and share information during a CCP crisis and that are involved in the CCP resolution planning, are expected to lead to additional guidance by the end of 2020³.

The FSB has also started work on the practical arrangements for the continuity of access of banks in resolution to a CCP or another FMI they are member of. This will allow the administrator of a resolved bank to adequately manage its resolution that typically requires access to FMIs⁴.

The CCP's ability to adequately handle a clearing member's default is essential from a prudential risk perspective. For OTC derivatives positions, the CCP re-establishes a balanced book by auctioning the positions of the defaulter to surviving clearing members. The adequacy of resources and the auction process attracted more attention in the wake of the NasdaqClearing clearing member default in September 2018. In June 2020, CPMI and IOSCO published a final paper on central counterparty default management auctions, a key element to handle a CCP participant's default. The report considers what constitutes a successful auction. The industry is being asked to make further progress on effective practices, including operational, auction governance and participation aspects⁵.

In the EU, EMIR, which sets out the obligations for market participants clearing derivatives⁶ besides the requirements for CCPs and their supervision, has been amended.

A first adaptation by the "EMIR Refit" Regulation⁷ entered into force on 17 June 2019. It mainly simplifies the derivatives reporting and clearing obligation requirements, but also requires CCPs to provide information on their initial margin models, including simulation tools, to their clearing members. Further, the European Commission now has the power to suspend the clearing obligation for selected derivatives contracts, for instance where markets become disrupted.

A second amendment by the EMIR 2.2 Regulation⁸ entered into force on 1 January 2020. It improves consistency of supervisory arrangements for CCPs established in the EU and enhances the EU's ability to monitor, identify and mitigate third-country CCP risks. While the primary role of the EU CCP's national competent authority is maintained, the supervision of CCPs is becoming more harmonised, via wider mandatory consultation of ESMA, and an enhanced role for the CCP supervisory college. Central banks responsible for EU currencies are also being given a bigger input. Furthermore, anticipating Brexit, the Regulation strengthens the third-country CCP authorisation and supervisory regime. It installs a direct ESMA supervision regime for systemic third-country CCPs, and even includes the possibility to require – via a Delegated Act – the relocation to the EU of so-called "substantially systemically important CCP" activities. Under EMIR 2.2, ESMA acts as a direct supervisor of third-country CCPs. In January 2020, the ESMA CCP Supervisory Committee started to operate. The Committee was established as part of the reform of the EMIR 2.2 review. In its "third-country CCP composition", it prepares ESMA decisions vis-à-vis third-country

1 Available at: <http://www.fsb.org/2015/09/2015-ccp-workplan/>.

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

3 See on this the FSB's 2019 Resolution report, available at <https://www.fsb.org/2019/11/2019-resolution-report-mind-the-gap/>.

4 See <https://www.fsb.org/2019/08/industry-workshop-on-continuity-of-access-to-fmis-for-firms-in-resolution/>

5 Available at <https://www.bis.org/cpmi/publ/d192.htm>

6 Most notably a clearing obligation applies, covering standardised interest rate swap contracts in the most relevant currencies, and index-linked credit default swaps. See further at <https://www.esma.europa.eu/regulation/post-trading/otc-derivatives-and-clearing-obligation>.

7 Regulation (EU) 2019/834 of 20 May 2019, available at <https://eur-lex.europa.eu/eli/reg/2019/834/oj>

8 Regulation (EU) 2019/2099 of 23 October 2019, available at <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R2099>

CCPs. The technical legislation for executing EMIR 2.2 is being further elaborated. In November 2019, ESMA published its technical advice on third-country CCP tiering, setting out what indicators ESMA has to consider to determine that a CCP is a so-called “Tier-2” CCP, i.e. systemically important for the financial stability of the EU or of one of its Member States. Also, it published technical advice on comparable compliance, that allows a Tier 2 third-country CCP to comply with EMIR requirements by complying with the regulations and requirements of its home country, if ESMA assesses them as satisfactory¹.

In December, ESMA also extended its recognition of the UK CCPs LCH Ltd, ICE Clear Europe Ltd and LME Clear Ltd for one year after a potential no-deal Brexit. This will prevent these CCPs from losing their authorisation as a Union CCP overnight². This means that EU clearing members will retain access to these UK CCPs during the post-Brexit transition period.

In January 2020, the European Commission, Parliament and Council started so-called “trialogues” to negotiate the final text of the proposed Regulation on CCP recovery and resolution. It sets out a framework for the recovery of a CCP, and the rules to ensure in resolution, the continuity of a CCP’s critical functions. It thereby avoids – via a loss allocation to the CCP’s clearing members, clients and shareholders – the use of taxpayers’ money to restructure and resolve the CCP. A final agreement is expected in 2020.

Prudential and oversight approach

In April 2019, ESMA published the framework of its third supervisory stress test for EU CCPs. The test focuses on both the counterparty credit risks and the liquidity risks that CCPs would face as a result of multiple clearing member defaults and simultaneous market price shocks³.

There is currently no CCP established in Belgium. However, CCPs are relevant for Belgian markets and clearing members, and settle in Belgian CSDs. The Bank continues to participate in seven EU CCP supervisory colleges as it meets at least one of the participation criteria⁴. Relevant CCPs include LCH Ltd in London that clears interest rate swaps, Eurex Clearing AG in Frankfurt that clears euro-denominated repos and LCH SA in Paris that clears the Euronext Brussels markets and euro repos. In addition, according to the same participation criteria, the Bank can take part in the third-country CCP supervisory college to be set up under EMIR 2.2, and where information will be shared on third-country CCPs⁵. For volume data on these three CCPs, see also Annex 3.

Supervisory priorities in 2020

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

Based on the FSB guidance, more national competent authorities are establishing cross-border crisis management groups for CCP resolution and plans for CCP resolution. In parallel, CCPs are enhancing their recovery rules that stipulate how to allocate default and non-default losses to stakeholders, including shareholders, clearing members and clients. Another ongoing priority is CCP operational risk management, and in particular the cyber risks faced.

1 See <https://www.esma.europa.eu/press-news/esma-news/esma-advises-ec-supervisory-regime-third-country-ccps>.

2 The ESMA decision, based on the also extended equivalence decision of the Commission, is available at <https://www.esma.europa.eu/press-news/esma-news/esma-extends-recognition-decisions-3-uk-ccps-in-event-no-deal-brexite>.

3 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>.

4 The NBB participates in the CCP supervisory colleges of Eurex Clearing AG (DE), LCH SA (FR), CC&G (IT), Euro CCP (NL), Keler CCP (HU) and LCH Ltd (UK) and ICE Clear Europe (UK).

5 This supervisory college will be quite relevant post-Brexit, to obtain information on the London based CCPs LCH Ltd and ICE Clear Europe.

Finally, new services or 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. Under the new EMIR 2.2 rules¹, the advisory powers of the college will expand. It is becoming easier for the college to escalate a file to ESMA for binding negotiation, and a college majority is now able to include specific guidance in its opinion, besides merely providing a positive or negative vote. Also, ESMA will provide a binding opinion to the CCP's national competent authority in a selected number of cases.

2.2 (I)CSDs

Changes in regulatory framework

The Law of 30 July 2018² put an end to the Belgian status of settlement institution as of 2020. This Belgian status has been replaced by the EU-wide status of central securities depository (CSD) pursuant to the CSD Regulation (CSDR)³. Therefore, Euroclear Belgium and Euroclear Bank needed to obtain their CSDR licence by the end of 2019 at the latest (see next section).

At the same time, the status of an institution assimilated to a settlement institution has been split into two new statuses. The first one is the status of institution providing support to Belgian CSDs. This status applies to Euroclear SA/NV (ESA), the parent company above the Euroclear (I)CSDs which provides services to these (I)CSDs (see Annex 2 for the organisation chart of the Euroclear group). The second new status is that of custodian bank, which applies to The Bank of New York Mellon SA/NV.

1 End March 2020, ESMA published draft regulatory technical standards for CCP colleges. See <https://www.esma.europa.eu/press-news/esma-news/esma-publishes-draft-regulatory-technical-standards-ccp-colleges>.

2 *Wet houdende diverse financiële bepalingen/Loi portant des dispositions financières diverses*.

3 Regulation (EU) No. 909/2014 on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No. 236/2012.

Summary of regulatory statuses of Belgian entities involved in the post-trade landscape

The Belgian institutions that are involved in the clearing, settlement and custody domain can have various regulatory statuses: CSD, institution providing support to Belgian CSDs, credit institution, financial holding or custodian bank. Institutions can combine several statuses. In addition to these statuses, they can be classified as systemically important institution, other systemically important institution (O-SII) or critical infrastructure.

Name	Regulatory status(es)	Main applicable frameworks relevant for the Bank's oversight and supervision*
Euroclear SA/NV ¹	<ul style="list-style-type: none"> ■ Institution providing support to Belgian CSDs ■ Financial holding 	<ul style="list-style-type: none"> ■ CPMI-IOSCO PFMI ■ Banking regulation
Euroclear Belgium ¹	<ul style="list-style-type: none"> ■ CSD 	<ul style="list-style-type: none"> ■ CPMI-IOSCO PFMI ■ CSDR
Euroclear Bank ^{1, 2, 3}	<ul style="list-style-type: none"> ■ CSD ■ Credit institution 	<ul style="list-style-type: none"> ■ CPMI-IOSCO PFMI ■ CSDR ■ Banking regulation
NBB-SSS ³	<ul style="list-style-type: none"> ■ CSD (no licence, as part of the central bank) 	<ul style="list-style-type: none"> ■ CPMI-IOSCO PFMI ■ CSDR (selected articles)
The Bank of New York Mellon SA/NV ^{1, 2, 3}	<ul style="list-style-type: none"> ■ Credit institution ■ Custodian bank 	<ul style="list-style-type: none"> ■ CSDR (reporting settlement internalisers) ■ Banking regulation

Source: NBB.

¹ Systemic financial institution (Art. 36/3 Organic Law).

² Other systemically important institution (O-SII) (Royal Decrees of 27 November 2015 and 18 December 2015).

³ Critical infrastructure (Law of 1 July 2011).

* A more elaborate list can be found in Annex 1 of this Report.

Systemic financial institutions' strategy and risk profiles are monitored closely (e.g. *ex-ante* non-objection requirement for strategic decisions). Institutions designated as O-SIIs have to keep higher capital buffers. The Bank is closely cooperating with critical infrastructures in the financial sector in order to strengthen their operational resilience.

ESMA has provided further guidance regarding CSDR Art. 23 on passporting and on the settlement discipline regime, the entry into force of which has been postponed to 1 February 2022¹. ESMA continues also to update its Questions & Answers on the CSDR².

The Shareholder Rights Directive II (Directive (EU) 2017/828, hereafter SRD II) – some provisions of which entered into force in June 2019, while others entered into force as of September 2020 – aims to encourage

¹ https://www.esma.europa.eu/sites/default/files/library/esma70-156-3490_final_report_-_csdr_rts_on_settlement_discipline_-_postponement_until_1_february_2022.pdf

² https://www.esma.europa.eu/file/21616/download?token=d8_lWUxK.

long-term shareholder engagement and stimulate good corporate governance. It includes requirements regarding remuneration in listed companies, related party transactions, transparency for institutional investors and asset managers, proxy advisors and identification of shareholders. It is this latter part where CSDs are involved. The goal of these provisions is to create a framework which allows issuers of listed companies in the EU to identify and communicate directly with their shareholders. Intermediaries (custodians and CSDs) must communicate information regarding shareholder identity including contact details and number of shares held without delay to the issuer. In addition, the intermediary should transmit through the chain, as soon as possible, from the issuer to the shareholder the information which the issuer is required to provide to the shareholder, to enable shareholders to exercise their rights (such as voting rights). Intermediaries also have to pass on to the issuer the instructions received from the shareholders related to the exercise of their shareholder rights. If there is a chain of intermediaries, this information has to pass through the chain all the way from the issuer to the intermediary who has a direct relationship with the ultimate shareholder and then back to the issuer. Intermediaries can charge fees for these services, but they have to be disclosed. They also must be non-discriminatory and proportionate in relation to the actual costs incurred for delivering the services.

Prudential and oversight approach

Considering that the Belgian status of settlement institution would cease to exist (see previous section), the Bank has focused on the applications for authorisation under the CSDR of Euroclear Belgium and Euroclear Bank.

Euroclear Belgium was authorised under the CSDR on 24 April 2019. Besides consulting the Eurosystem (as relevant authority as defined in the CSDR) and the Belgian Financial Services and Markets Authority (FSMA), the Bank coordinated its compliance assessment with the authorities of Euroclear France and Euroclear Nederland, which use the same platform as Euroclear Belgium.

Euroclear Bank was authorised by the Bank under the CSDR on 3 December 2019 to provide core services as a CSD and to provide banking-type ancillary services. In addition, the interoperable link with Clearstream Banking SA (called the “Bridge”) was authorised by the Bank. Besides consulting the FSMA for specific items¹, the Bank also consulted the central banks issuing the relevant EU currencies (at the moment of consultation, these were EUR, GBP and DKK for Euroclear Bank) for the CSD licence as required by the CSDR. In addition to those, the Luxembourg Commission de Surveillance du Secteur Financier (CSSF) was consulted regarding the Bridge. For the licence to provide banking-type ancillary services, the Bank had to consult 22 authorities from the EU.

¹ Rules on conflicts of interest, record-keeping, 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.

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, Euroclear Bank and Euroclear Belgium. The table below provides the list of authorities and the rationale for having a cooperation arrangement with them.

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, Finansinspektionen; UK: Bank of England, Financial Conduct Authority)	Multilateral cooperation with regard to shared services provided by the parent holding company of the Euroclear Group (I)CSDs (Euroclear SA), as 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 on specific aspects of Euroclear Bank relevant for euro area financial stability
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)	Cooperation on the oversight and supervision of the ICSDs Euroclear Bank and Clearstream Banking Luxembourg, under Responsibility E of the PFMI
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.



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 euros in central bank money, the Eurosystem (represented by the Bank) is considered as a relevant authority as well. For Euroclear Bank, this also included Bank of England and Danmarks Nationalbank at the moment of authorisation. For this category of relevant authority (central banks in the EU 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 in the EEA. ESMA publicly discloses the list of relevant authorities¹.

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 calculating 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 place² and (ii) the substantial importance of a CSD for a host MS³.

1 https://www.esma.europa.eu/sites/default/files/library/esma70-151-887_csd_list_of_relevant_authorities_art_12.pdf.

2 https://www.esma.europa.eu/sites/default/files/library/esma70-708036281-66_csd_guidelines_on_relevant_currencies_0.pdf.

3 https://www.esma.europa.eu/sites/default/files/library/esma70-708036281-67_csd_guidelines_on_substantial_importance_of_a_csd_0.pdf.



Consultation in the context of the CSDR	Rationale for consultation
National consultation	
Euroclear Bank / Euroclear Belgium	
<i>CSD services</i>	
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	
<i>CSD services</i>	<i>Central bank of issue of the most relevant currencies in which settlement takes place².</i>
Eurosystem, Bank of England, Danmarks Nationalbank	Calculation methodology ³ : <ul style="list-style-type: none"> the relative share of each EU 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 EU currency compared to the total value of A/P settlement instructions settled in that currency across all CSDs in the EU, provided that such share exceeds 10 %
<i>Banking-type ancillary services</i>	<i>The following authorities are involved in the authorisation of the CSD⁴</i>
Eurosystem, Bank of England, Danmarks Nationalbank	<ul style="list-style-type: none"> Relevant authorities
Commission de Surveillance du Secteur Financier (CSSF)	<ul style="list-style-type: none"> Competent authority for the CSDR in the MS where the CSD has established interoperable links with another CSD
Competent authorities from twenty MS in the EU	<ul style="list-style-type: none"> 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 investors⁵ 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 EU⁶ 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
Euroclear Belgium	
<i>CSD filing</i>	
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.

The CSDR transposed the PFMLs into EU law and introduced some new requirements for (I)CSDs in some areas. For example, (I)CSDs providing banking-type ancillary services need to have sufficient qualifying liquid resources to withstand the default of the two participants to which they have the largest exposures (the PFMLs require enough resources to withstand the default of the largest one). With regard to credit risk management, the CSDR prescribes more explicitly what kind of securities can be accepted as collateral and introduces a hierarchy to use very liquid securities of high quality first. While high-quality collateral significantly reduces the residual credit risk an (I)CSD is faced with, extreme market shocks could reduce the value of the collateral beyond the prediction of valuation models that determine the “haircut” on the collateral value. Residual credit losses could also occur in the event of default of a cash correspondent where cash is (temporarily) held in an unsecured way. (I)CSDs need to have plans that specify how potentially uncovered credit losses are allocated. Potential losses can typically be allocated to two types of stakeholders: the shareholders and the participants. The shareholders are the ones that benefit when profits are made. Should the (I)CSD be confronted with major losses, shareholders could recapitalise the (I)CSD, but there is generally no upfront commitment to do so. The rules of the system could also allocate (part of) such losses to the participants (as is customary for CCPs) who are the ones that benefit from the services that the (I)CSD provides (including the provision of credit facilities). When designing a loss-sharing mechanism with participants, certain aspects need to be considered carefully. Decision-takers in (I)CSDs need to have the right incentives in order to prevent shareholders from always keeping the profits in favourable times but distribute losses to the participants in adverse situations. Another aspect to consider is the fact that other (critical) FMIs may be participants in an (I)CSD. Pushing losses onto them may therefore worsen the potential systemic impact.

As soon as Euroclear Belgium and Euroclear Bank were authorised, a formal process started to obtain non-objections from the authorities of host Member States where they have set up a branch or under whose law they currently issue, or intend to issue, securities, as required in CSDR Article 23.

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 2019, Euroclear Bank had 1 657 participants located worldwide. Its participant base consists mainly of non-domestic participants, including 92 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 2020, Euroclear Bank is connected to more than 50 foreign CSDs as investor ICSD in these 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. Securities can be settled against payment in a Euroclear settlement currency which can be different from the denomination currency. Denomination currencies are used as units of account for securities balances but not necessarily for payment transactions.

At the end of 2019, the value of securities deposits held on Euroclear Bank's books on behalf of its participants amounted to € 14.8 trillion equivalent (up from € 13.5 trillion in 2018). After EUR (47 %), USD is the main denomination currency (30 %), 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 2019 in Euroclear Bank amounted to 116.3 million (up from 107.0 million in 2018). In value terms, this represents € 544.6 trillion (up from € 525.7 trillion in 2018). 61 % of settlement turnover, free of payment and against payment transactions, was denominated in EUR, after USD (18 %) and GBP (9 %). 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 tri-party 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 2019, at group level, the average daily value of triparty collateral managed by the Euroclear (I)CSDs had reached € 1.3 trillion equivalent (up from € 1.2 trillion in 2018).





The interconnection of the different market infrastructures is a necessity for the exchange of financial flows, but this interconnectivity is also a major risk in the event of a problem at one of the elements of the chain, which could impact other FMIs. Hence, cyber resilience continues to be a top priority for the Bank in its oversight activity with Belgian (I)CSDs. In particular, implementation of the SWIFT Customer Security Programme (CSP) framework continued to be monitored in 2019.

The ESA Cyber Resilience Task Force, which includes central banks and securities regulators of all Euroclear Group entities, and is chaired by the Bank, monitors the progress of the Euroclear Group in the implementation of its cyber security strategy and related projects. The governance of the (I)CSD in the cyber domain, and the interactions with Risk Management (2nd Line of Defence) and Internal Audit (3rd Line of Defence) is also an important point of attention in this context.

Also, in 2019, Euroclear participated in

- the second ESCB Cyber Assessment Survey (assessment of cyber security maturity of FMI, based on the CPMI IOSCO Cyber Resilience guidance, dated June 2016) which allowed to position Euroclear among peers:
- an anonymous peer-benchmarking exercise for implementation of business continuity planning (BCP) with 37 other peer FMIs, under the coordination of CPMI and IOSCO. The goal was to review the consistency of implementation of the relevant Principles (related to BCP) of the PFMI.

The Bank contributed to the analysis and evaluation of the two above-mentioned exercises.

In 2019, the oversight team monitored the NBB-SSS's project to offer DVP settlement in foreign currencies for trades as well as for corporate actions in a fully automated way as of Q2 2020. In other words, the NBB-SSS will support the settlement of the cash leg in a foreign currency relating to securities denominated in foreign currencies registered in the NBB-SSS. This eliminates principal risk for participants related to securities denominated in foreign currencies, even though these securities make up only a small fraction of the NBB-SSS's securities depot.

With regard to CSDR settlement discipline, Belgian (I)CSDs' preparations for installing the penalty regime between participants are ongoing. The T2S penalty mechanism will provide CSDs daily with the fines to collect and distribute per participant.

With regard to T2S, a total of 22 CSDs are now connected to the pan-European platform, covering 20 national markets. Since the Danish krone (DKK) connection from 29 October 2018, T2S has become a multi-currency platform, offering the possibility of DVP settlement in another currency than the euro. As part of its regular activities, the T2S Oversight function assesses incident occurrence and monitors changes in statistical indicators and other issues with an impact on the smooth functioning of T2S which may be relevant from an oversight perspective, such as management of operational risks by T2S. These activities are ultimately designed to identify any potential impact on the safety and efficiency of T2S or its compliance with the relevant requirements of the PFMI. In 2019, the Eurosystem T2S oversight function finalised a comprehensive evaluation of T2S compliance with the PFMI on which the authorities involved in the T2S Cooperative Arrangement were consulted.

Finally, the Bank is also following up the innovations in the settlement domain such as distributed ledger technology (DLT)¹. In 2019, there was an initiative by the European Investment Bank (EIB), Euroclear, Banco Santander and EY with regard to an end-to-end blockchain solution for the exchange of information between parties regarding the issuance of European Commercial Paper (ECP)². The issuance and settlement itself would remain on Euroclear Bank's existing system. Crypto assets issued on DLT networks or tokenisation platforms have the potential to disrupt the post-trade areas of the securities industry. However, there are considerable challenges before these innovations can be brought into practice in the post-trade industry. A paper by the International Securities Service Association (ISSA)³ discusses some of these challenges and outlines recommendations and best practices. Among the challenges a CSD faces when it wants to serve security tokens issued, traded and settled on DLT are legal issues⁴.

1 More background information on DLT in the field of FMIs can be found in the Financial Market Infrastructures and Payment Services Report 2017 ("Enabling technologies in financial market infrastructures and payment services innovation: An overseers' perspective on opportunities, risks and policy").

2 "EIB, Euroclear, Banco Santander & EY developing blockchain solution", 19/06/19, available at <https://www.euroclear.com/newsandinsights/en/press/2019/mr-11-Euroclear-developing-Blockchain-solution.html>

3 "New ISSA industry paper on DLT & Crypto Assets", 14/11/2019, available at <https://www.euroclear.com/newsandinsights/en/Format/Whitepapers-Reports/ISSA-Crypto-Assets-paper.html>

4 An article by Bart Garré and Sofie Van de Velde discusses this aspect: "Can securities be issued, traded and settled on DLT? Legal considerations from a CSD's perspective", *Droit bancaire et financier/Bank- en Financieel Recht*, Volume 2019, Nr. 2, available at <https://www.jurisquare.be/en/journal/bfr/2019-2/can-securities-be-issued-traded-and-settled-on-dlt-legal-considerations-from-a-csds-perspective/index.html#page/130/search/>

The evolution of new technologies such as the virtualisation or the use of cloud computing are also being closely monitored from an operational risk management perspective.

Supervisory priorities in 2020

Once a CSD has been authorised under the CSDR, it is subject to a review and evaluation process by the competent authority of that CSD. As both Euroclear Belgium and Euroclear Bank were licensed in the course of 2019, the review and evaluation process by the Bank started in 2020. As competent authority, it will assess their compliance with the CSDR on a yearly basis.

For Euroclear Belgium, this review and evaluation process is coordinated – like the CSDR authorisation process before – with the FSMA and authorities of Euroclear France and Euroclear Nederland. Focus is put on the CSD's activities and any substantive changes made during the review period. New statistical data reporting on Euroclear Belgium's business based on CSDR methodology will also be made available as from the review and evaluation process. As foreseen in the CSDR, the Bank will consult other relevant authorities: i.e. the Eurosystem in the case of Euroclear Belgium.

For Euroclear Bank, having been licensed in December 2019, the process will only be initiated by the end of 2020. The review and evaluation itself will be conducted by the Bank¹ in early 2021. The Bank will also further work on loss-sharing arrangements with participants/counterparties as this is a relevant requirement in several frameworks. Other priorities, mainly in the area of banking-type ancillary services provided by Euroclear Bank, are a comprehensive assessment of the risks associated with voluntary end-of-day long cash balances of participants and a review of the methodology, scope and frequency of the liquidity stress tests. Ancillary services such as securities lending will also be analysed against PFMI and CSDR requirements.

In order to avoid credit risks on cash correspondents, the Bank continues to support Euroclear Bank's efforts to open central bank accounts for foreign currencies where it has not yet done so. The ability to access such central bank accounts – and the conditions theretofore doing so – depend on the policy of local central banks.

As NBB-SSS is being used by the Eurosystem for the mobilisation of collateral in the framework of implementation of monetary policy operations, the Bank will conduct a review and evaluation of NBB-SSS against the CSDR requirements which are relevant from a user perspective and consult the Eurosystem in this context.

For all (I)CSDs established in Belgium, cyber resilience continues to be closely monitored by the Bank, in particular the projects aiming to further strengthen the (I)CSDs' security position. In this area, the Bank cooperates with the Euroclear Group authorities. The current cooperative framework arrangement between Euroclear Group regulators (overseers/securities regulators) will also be revised to take into account the impact of the CSDR.

¹ For the aspects mentioned in the footnote on page [25], the Bank will consult the FSMA.

COVID-19 impact on Belgian (I)CSDs

As the coronavirus crisis erupted, Belgian (I)CSDs activated their BCP arrangements, and initiated a general working from home arrangement for the staff. Some with offices in Asia had already activated such arrangements for these locations at the beginning of the year.

With the coronavirus crisis leading to greater volatility and trading volumes in markets, CCPs and (I)CSDs found themselves dealing with a significant increase in transactions to be processed. As there are strict capacity management requirements for FMI, the Belgian (I)CSDs absorbed these peak volumes without any problem.

Some of their participants struggled to cope with the combination of higher transaction volumes and working-from-home arrangements for their staff. In some cases, this was due to the fact that some of the back offices were located in a country that abruptly went into lockdown (or back offices had outsourced a significant part of their operations to providers located in such countries) and where the BCP did not cater for such a sudden lockdown. This led to an increased number of transactions that did not settle on the intended settlement date (so-called “failed transactions”). Euroclear Bank exceptionally opened a window for introducing instructions on a Saturday to allow the participants that were affected, to enter instructions for processing in order to reduce the backlog of unmatched/unsettled instructions.

For supervisory and oversight activities on (I)CSDs, physical meetings have been replaced – since the start of the COVID crisis – by virtual interactions, including for international cooperative arrangements.

2.3 Custodians

Changes in regulatory framework

According to Article 9(1) of the CSDR, settlement internalisers have to report to the competent authorities where they are established on a quarterly basis the aggregate volume and value of all securities transactions that they settle outside securities settlement systems (see box 7 in the Financial Market Infrastructures and Payment Services Report 2019 for more information). In 2019, several settlement internalisers in Belgium have started reporting as required by the CSDR.

Prudential approach

As a global custodian, The Bank of New York Mellon (BNY Mellon) operates according to a “follow the sun” model that enables client transactions and related services around the world to be continuously processed, thanks to the global footprint it has established with entities spread around the globe, working on common platforms and multiple intra-group outsourcing arrangements.

In line with this business model, the NBB's supervisory work in the Joint Supervisory Team (JST) in 2019 was mainly focused on assessing compatibility of the structuring of the various streams that are relevant for BNYM SA/NV within the new context and related supervisory requirements resulting from Brexit.

The core principles guiding these assessments can be found in the Operational Brexit Guidance published on the ECB's website¹.

When adjustments to existing streams were required (including expanding the product and service offering of BNYM SA/NV for EU clients), the JST considered the expected changes and assessed the proposed projects from a legal, operational as well as governance vantage point. The impact on the bank's financial ratios, internal control system and risk profile were of course integrated into the supervisory assessments.

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

BOX 6

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

BNY Mellon, a banking group incorporated in the US, is one of the largest custodian banks in the world in terms of assets under custody (\$ 37.1 trillion as at December 2019, up by 12 % on last year). It is a global systemically important bank (G-SIB), providing asset and investment management services to institutional customers. BNYM SA/NV, the Belgian subsidiary, provides asset services mainly and acts as the BNY Mellon group's custodian for T2S markets and as the custodian for EU customers. BNYM SA/NV has a non-bank subsidiary in Germany and branches in Luxembourg, the Netherlands, Germany, France, Ireland, Italy and the UK, through which it operates in these local markets. BNYM SA/NV qualifies as an other systemically important institution (O-SII), as assessed by the NBB based on the relevant EBA guidelines.

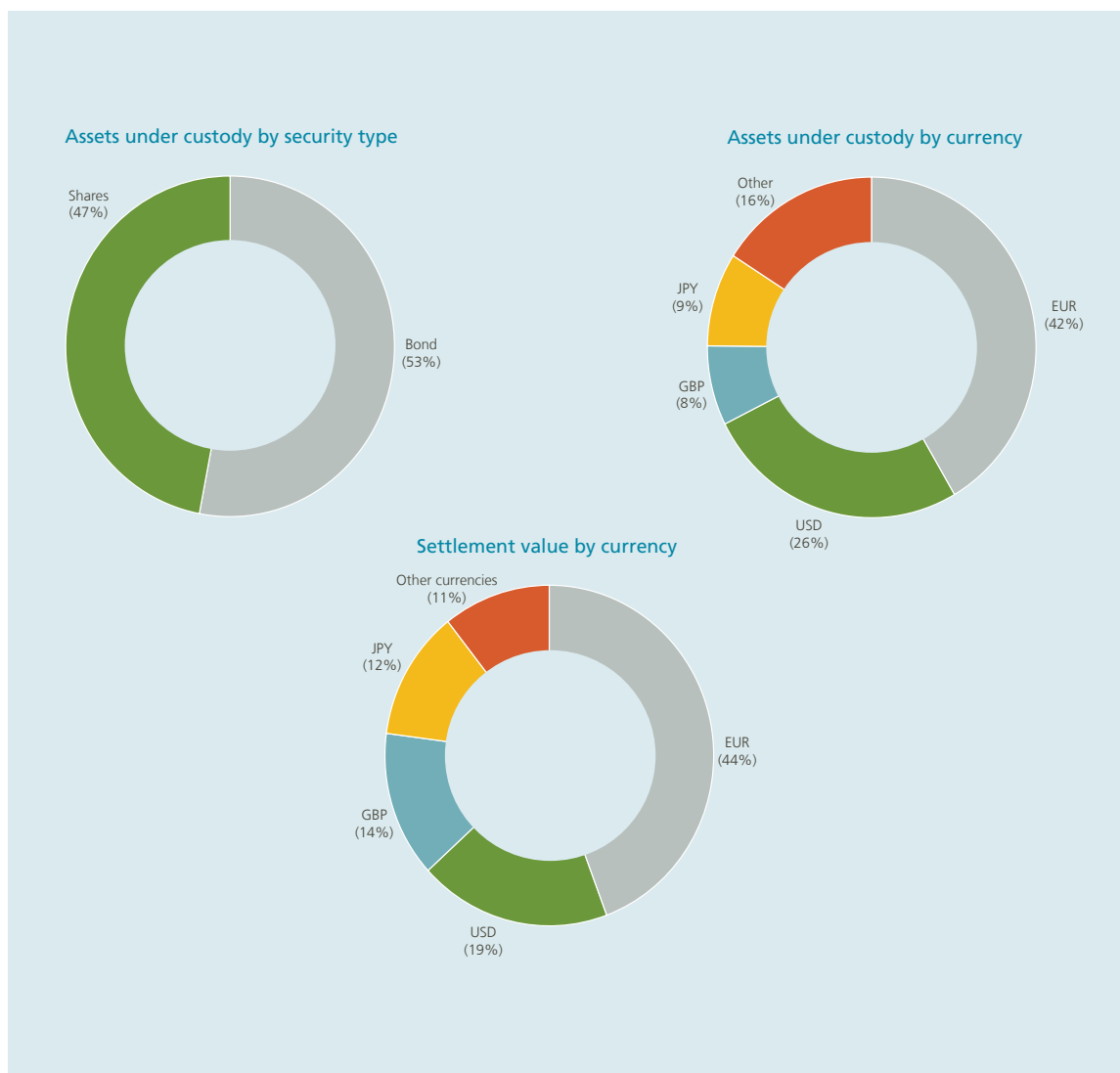
By the end of 2019, BNYM SA/NV served more than 750 international, institutional customers¹ on whose behalf it held € 2.8 trillion equivalent assets under custody, denominated in more than 75 different currencies². The majority of these assets are denominated in euro (42 %), followed by USD (26 %), JPY (9 %) and GBP (8 %). 53 % of these assets are bonds and 47 % of these assets are shares. In terms of settlement activity³, BNYM SA/NV processed about 13.8 million transactions worth € 37.3 trillion equivalent in 2019. The main currencies are EUR (44 %), USD (19 %), GBP (14 %) and JPY (12 %).

¹ Compared to last year, client numbers are now reported at the parent company level.

² Eligible currencies include AED, ARS, AUD, BDT, BGN, BHD, BMD, BRL, BWP, CAD, CHF, CLP, CNY, COP, CRC, CZK, DKK, EGP, ETB, EUR, FKP, GBP, GEL, GHS, GMD, HKD, HRK, HUF, IDR, ILS, INR, ISK, JPY, KES, KRW, KWD, KYD, KZT, LBP, LKR, MAD, MUR, MXN, MYR, MZN, NAD, NGN, NIO, NOK, NZD, OMR, PAB, PEN, PGK, PHP, PKR, PLN, PYG, QAR, RON, RSD, RUB, SAR, SEK, SGD, THB, TND, TRY, TWD, TZS, UAH, UGX, USD, UYU, VES, VND, XOF, ZAR, ZMW, ZWL.

³ Value of BNYM settlement activity is based on receipt and delivery instructions.





Besides this important stream of supervisory work, the NBB also reviewed and authorised (both in conjunction with the ECB and autonomously under the custodian bank status) important restructuring operations under the group's operating model restructuring initiative launched several years ago. The objective of this multi-year initiative is to simplify the group's structure and to ensure enhanced relationships between the group locations, client contractual framework and client assets under custody in both an ongoing and resolution perspective.

Two operations can be highlighted in 2019 in that regard: the takeover of an Irish group entity by BNYM SA/NV and the closing of BNYM Brussels branch.

Lastly, taking into account the fact that BNYM's business model shares several characteristics with that of FMI, a continuous focus on the IT and operational resilience of the entity, as well as its recovery and resolution planning, is integrated into the supervisory planning.

Supervisory priorities in 2020

The supervisory planning for BNYM SA/NV in 2020 will ensure continuity with the tasks performed last year.

Readiness for Brexit will continue to be a core aspect of the supervisory work, with focus gradually shifting from so-called “day-1” solutions (the solutions banks have put in place in the period between the ratification/entry into force of the Withdrawal Agreement and the end of the transition period, i.e. February 2020-December 2020) to “day-2” solutions (the solutions banks have put in place to do business in Europe after 31 December 2020).

The firm’s resilience will continue to be monitored from an IT and operational perspective. The enhancements made to the technical infrastructure through internal innovation or collaboration with FinTech companies and third-party providers will be closely followed to ensure their compliance with European regulations.

BOX 7

How custodians have been dealing with the coronavirus crisis

The COVID-19 pandemic has resulted in higher on-balance sheet leverage for custodians. Owing to the pandemic-induced market turmoil, investors have decided to keep a larger extent of their funds in cash, possibly by liquidating positions but more generally by not immediately rolling over part of their securities investments at redemption date. Custodians being considered as safe havens by their clients, based on their business model that implies that they do not intensively engage in risk-taking activities for own account, these clients decided accordingly to park more of their cash in their accounts with the custodians.

The extra leverage could create additional credit and liquidity risks challenges for the receiving entities. The additional cash needs to be reinvested in high-quality liquid assets in line with the typical nature of custodians’ short-term and liquid liabilities, and without significantly increasing the credit risk profile of the custodian.

The COVID-19 pandemic has also resulted in increased amounts of transactions (securities purchases as well as FX) in the first phase of the crisis. Additional transactions have a positive impact on the fee income which is the major source of revenue for custodians, but other parameters – which evolved sharply due to the pandemic – also impact custodian bank revenues as the evolutions in securities prices or the interest rates. Besides euro area interest rates that have been at historically low levels for some years, other markets, especially the US, have seen significant drops in interest rates.

Custodians are a central part in the functioning of globalised financial markets. To be able to offer services that meet client expectations and ensure stability in the functioning of markets, custodians have to build a high level of resiliency by several means, amongst which fall-back capabilities between regional operational centres. These capabilities, coupled with secured remote working infrastructure proved reliable in the current circumstances, even when used at unprecedented levels.

3. Payments

The Bank has a broad responsibility in the area of payments and adopts the role of both overseer and prudential supervisor, as illustrated in chart 4 below. These approaches are complementary: while oversight concentrates on the sound and safe functioning of payment systems, payment instruments¹, payment schemes² or other payment infrastructures, prudential supervision pursues safe, stable and secure payment service providers 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 (LVPS) 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. The CEC is the domestic retail payment system (RPS) processing domestic payments between Belgian banks.

The Bank also participates in the cooperative oversight framework of CLS, a payment-versus-payment (PVP) settlement system for foreign exchange (FX) transactions. The U.S. Federal Reserve is the lead overseer and supervisor of CLS. 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 NBB).

Section 3.2 deals with the prudential supervision of payment institutions (PIs) and electronic money institutions (ELMIs) – a part of the PSP sector which offer their services in competition with the incumbent PSPs (mainly banks). 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 acquirer³ and processor of retail payment instruments 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.

Section 3.4 covers the three payment card schemes overseen by the Bank: the domestic Bancontact scheme and the international Maestro and Mastercard schemes (these latter two being operated by Mastercard Europe SA/NV as governance body).

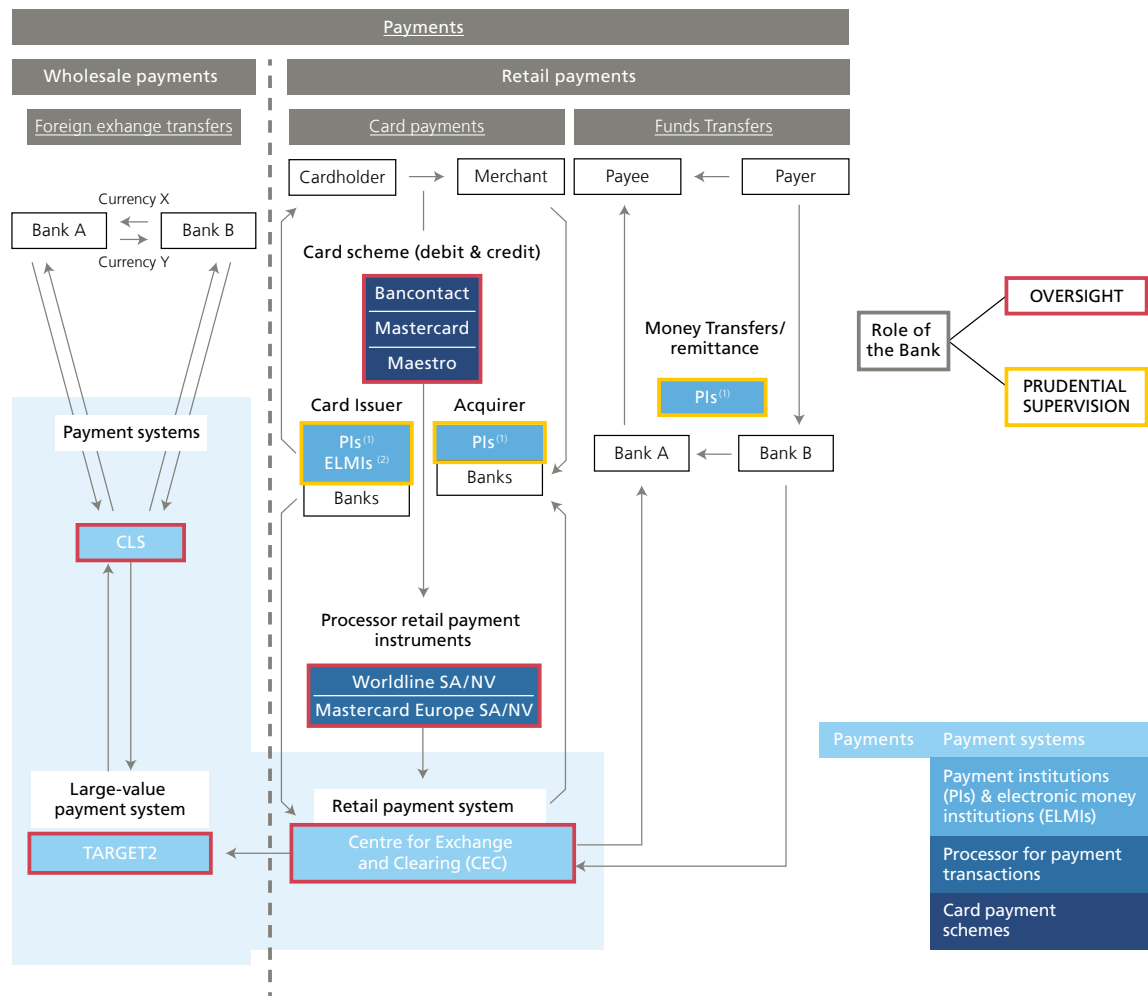
1 A payment instrument is an instrument to execute payments such as cards, credit transfers and direct debits.

2 A payment scheme is a set of rules, practices, standards and/or guidelines for the execution of payment transactions.

3 Acquiring card payments is a service whereby a payment service provider contracts with a payee (merchant) to accept and process payment transactions, and guarantees the transfer of funds to the payee (merchant). The processing part is often performed by another entity.

Chart 4

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



1 Payment institutions (PIs).

2 Electronic money institutions (ELMIs).

Impact of COVID-19 on the payments sector

Given the widespread nature and ubiquity of payments in economic life, both the Belgian and international payments market has been significantly and profoundly affected by COVID-19. Even though existing payment infrastructures and payment service providers were able to maintain their operational continuity, the pandemic, together with the subsequent government measures, did generate a substantial and asymmetric shock on the processed number and value of processed transactions for the industry. Moreover, due to the diverse means of payment available for end users, ranging from both cash to credit transfers, this effect was more pronounced for certain service providers than for others.

Based on additional, *ad-hoc* reporting for the sector since the early phase of the government's measures in Belgium, the Bank has been able to estimate a general decline of over 30 % in the value of processed card payments within Belgium at the point of sale (i.e. in-store payments) during the first month of the lockdown, compared to the same period of the previous year. This observation is in line with the figures recorded in other European countries. Yet, Belgian e-commerce card transactions surged during this period with an increase of over 20 %, both in terms of value and volume. This trend was probably due to a shift in consumer spending habits during the initial phase of the measures announced by the government.

Next to this, cash intensive payment services and travel related payment solutions were significantly hit. For example, both the number and value of transactions for certain cash-based money remittance providers in Belgium declined by more than 50 % in the first week of the lockdown period, compared to the same period the previous year. But cross-border payments based on credit transfers rose significantly for specialised payment institutions over this period.

As these figures illustrate, COVID-19 has left a profound and diverging impact on existing payment flows and payment habits. For example, the limit for making a card payment without strong customer authentication (SCA) was lifted from € 25 to 50 for one-off payments with a cumulative threshold raised from € 50 to 100. This increased the number of contactless payments considerably and will probably further enhance the growth and establish this payment habit. In view of the ongoing nature of the pandemic, the Bank expects the effect of this shock on both individual actors and the broader payments landscape to continue for the foreseeable future.

3.1 Payment systems

Changes in regulatory framework

There were no changes in the Belgian regulatory framework in the course of the period running from April 2019 to April 2020.

Oversight approach

The Bank is responsible for the oversight of the CEC, the Belgian domestic retail payment system. The main change in the system was the launch, on 4 March 2019, of a platform developed and run by the French company STET enabling the processing of instant payments (IP). Although the technical platform supporting IP processing and settlement is technically separated from the existing one and has specific features (e.g. settlement based on pre-deposited amounts held by the system on a technical account in TARGET2), it is integrated into the existing automated clearing house as an additional functionality and not as a new system.

The Bank as overseer has been monitoring the development of the IP platform and its specific features such as the establishment of a technical account in TARGET2. Despite the demanding nature of the system, which requires availability in real time not only of the central platform but also the sending and receiving banks, as well as their quick interaction (the payment must be finalised in less than 5 seconds) for the execution of a payment, the IP functionality started smoothly with no significant incidents. The volumes processed are increasing steadily. In 2019, 60 million IP operations were processed with peaks at more than 400 000 operations per day. By the end of 2019, IP represented about 12 % of all credit transfers processed by the system and, on the whole year, about 0.4 % of the total volume. Interoperability with other IP systems should be the next step for the CEC IP. The systems to be connected are the French IP system¹ as well as the pan-European systems TIPS and RT1. From a technical perspective, the necessary features are already in place at system level.

With the ECB as the lead overseer, the Eurosystem is responsible for oversight of three Systemically Important Payments Systems (SIPS): TARGET2, EURO1 and STEP2. They are overseen on a cooperative basis along with the national central banks in the Eurosystem. During the 2019 classification exercise of payment systems, the Eurosystem concluded that MCE ought to be listed as another systemically important payment system with the ECB and the Bank, as joint lead overseers (see section 3.4).

The CLS Oversight Committee has monitored, among others, CLS' projects to further reduce risks in the FX markets. CLSClearedFX is a service that allows CCPs and their clearing members to safely and effectively mitigate settlement risk when settling cleared FX products. CLSNet is a bilateral payment netting calculation solution, operating on a distributed ledger technology (DLT) platform. CLSNow enables intraday PVP settlement (provided that the payment systems of both currencies are open) – currently transactions are settled gross on a bilateral basis and for a limited number of currencies.

Supervisory priorities in 2020

In 2020, the Bank will continue to pay specific attention to the development of the CEC's cyber resilience. The Cyber Resilience Oversight Expectations for FMIs (CROE)² will be used as standard to assess the CEC's maturity in this field. Future developments in the CEC platform (IP and legacy) will also be covered in the oversight framework.

¹ The same IP technical platform is used by the French market, but the Belgian and French markets are separate user groups, and it is not yet possible to carry out IP between them.

² Link available here: https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf.

3.2 Payment Institutions and Electronic Money Institutions

Changes in regulatory framework

In 2018, the second Payment Services Directive 2015/2366 (PSD2)¹ was transposed into Belgian legislation. PSD2 aims to encourage innovation and competition by enabling new players to offer new types of payment services on the market. The Directive also aims for simpler, safer and more efficient payment transactions within Europe through such things as the introduction of the concept of strong customer authentication.

PSD2 was transposed into Belgian law via two pieces of legislation. The first one, the Law of 11 March 2018², contains the prudential aspects of PSD2 and falls within the competence of the Bank. This Law also repeals and replaces the Law of 21 December 2009. The second piece of legislation, the Law of 30 July 2018 amending Book VII of the Code of Economic Law, contains consumer protection and conduct of business rules and falls within the competence of the Federal Public Service Economy.

In 2019, the last Royal Decree³ within the framework of the Law of 11 March 2018 was issued. This Royal Decree stipulates the regulations of the Bank on own funds requirements for electronic money institutions. More specific, the Decree requires that the prudential own funds of electronic money institutions must at any time be at least equal to the maximum of € 350 000 or the sum of the required equity calculated on the basis of the issued electronic money, which equals to 2 % of the average outstanding money, and the provided payment services, for which the regulatory framework defines three different methods (A, B or C).

In order to develop a coherent legal framework at Community level, the European Commission also conferred 12 mandates on the EBA within PSD2. These mandates consist of five RTSs⁴ (Regulatory Technical Standards), which are of direct effect across the European Economic Area, and 7 Guidelines, which were implemented in the Bank's supervisory framework via Circulars issued in 2018 and 2019. An important element of the Law of 11 March 2018 relates to the requirement for institutions to remain responsible for the fulfilment of all its obligations of its outsourced functions, activities or operational tasks. In particular, outsourcing may not lead to the quality of internal control being compromised, nor to any unnecessary increase in operational risk.

In line with this, the EBA issued a set of guidelines on outsourcing on 25 February 2019. These were implemented in Belgium by the Circular of 19 July 2019⁵, which is applicable to all institutions under supervision of the Bank, including payment institutions and electronic money institutions. The Circular sets out a transitional period for existing outsourcing agreements until 31 December 2021 and requires institutions to report the following to the Bank: i) an outsourcing register, ii) planned outsourcing of critical/important functions, iii) a notification when outsourced functions become critical/important and iv) a notification when there are material changes or critical incidents concerning outsourcing agreements.

1 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No. 1093/2010, and repealing Directive 2007/64/EC, OJ. 23 December 2015, L 337, 35-127.

2 The 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).

3 Royal Decree of 21 March 2019 approving the rules of the National Bank of Belgium on own fund requirements of electronic money institutions.

4 The RTS on home-host cooperation has been adopted by the EBA and been submitted to the European Commission. The final RTS still needs to be published by the European Commission.

5 Circular 2019_19 on the guidelines of the European Banking Authority of 25 February 2019 on outsourcing.

Regulatory Technical Standards on SCA and CSC

A key mandate conferred on the EBA within the context of PSD2 relates to the drafting of regulatory technical standards on strong customer authentication (SCA) and common and secure communication standards (CSC)¹. These RTS on SCA & CSC came into force 18 months after the entry into force of PSD2, i.e. on 14 September 2019. They form the key piece of legislation in rendering PSD2 operational in the payments landscape as it contains both the detailed requirements on what constitutes “strong customer authentication” and any exceptions to the rule, as well as the rules on rendering access to payment accounts possible for payment initiation and account information service providers.

(i) Strong Customer Authentication: ongoing work

In June 2019, the EBA published an Opinion on the elements of strong customer authentication under PSD2 in which clarifications were provided to the market concerning what factors may constitute inherence, possession or knowledge elements of SCA. The Opinion furthermore clarified the concepts of dynamic linking and independence of elements that are an integral part of SCA.

By the time this Opinion was handed down on 21 June 2019, it had become apparent that the EBA's interpretation of which factors constitute an authentication solution that may be considered as SCA posed significant issues for the card payment industry. The concerns raised by the industry were specific to online commerce (e-commerce) with payment cards.

The first concern related to authentication solutions for payment cards in online commerce being still based on the use of the card details (as printed on the payment card), sometimes combined with an SMS one-time password (OTP) or a biometric authentication solution on a mobile device (e.g. a fingerprint or FaceID). As the above-mentioned Opinion stated unequivocally that printed card credentials do not constitute any factor in strong customer authentication, the issuers of such payment cards (credit institutions, payment and electronic money institutions) needed to find alternative authentication solutions that can ensure a continued two-factor authentication that meets the requirements of strong customer authentication under the RTS on SCA & CSC.

The second concern related to the use of the nine exceptions to the rule of strong customer authentication listed in the RTS on SCA & CSC. These exceptions were purposefully crafted in order to ensure the smooth working of electronic payments, including online commerce with payment cards, and thus for cases where the application of SCA was not considered by law to provide additional value in terms of reducing fraud or ensuring security. Examples of this include the use of contactless payments at a point of sale under a certain amount in euro, low-value transactions and transaction risk analysis when the fraud rates are sufficiently low.

¹ Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication (hereafter: RTS on SCA & CSC).



However, in order to render the use of these exceptions operational in the sphere of online commerce with payment cards, it requires smooth communication of the desire to leverage a particular exception between online merchants' websites, their payment card acquirers and the issuers of those payment cards. Before the summer of 2019, it became clear that this would not be achievable by 14 September 2019.

The combination of these two concerns with a strict adherence to the entry into force of the SCA requirements on 14 September 2019 had the potential to negatively impact EU customers who made use of payment cards in online commerce. The changes SCA introduces require online merchants to make changes on their websites (in order to support the exceptions to SCA) as well as customers to change the way they authenticate with their payment card in the online environment. They also require card issuers to issue their customers with SCA-compliant cards. It was considered paramount by regulators across the EU that customers would continue to be able to make payments, including online, with payment cards, without suffering interruptions.

In response to these two industry concerns, the EBA's aforementioned Opinion provided the option to each competent authority (CA) under PSD2 "on an exceptional basis and in order to avoid unintended negative consequences for some payment service users after 14 September 2019, to work with PSPs and relevant stakeholders, including consumers and merchants, to provide limited additional time to allow issuers to migrate to authentication approaches that are compliant with SCA, and acquirers to migrate their merchants to solutions that support SCA". The EBA further specified that this supervisory flexibility is available under the condition that PSPs have set up a migration plan, have agreed the plan with their CA, and execute the plan as quickly as possible. CAs should also monitor execution of these plans to ensure swift compliance with PSD2 and the EBA's technical standards and to achieve consistency of authentication approaches across the EU.

Over the 2019 summer period, the Bank conducted an analysis of the state of readiness of the Belgian market, concluding that the main issues were related to the second concern listed above and mainly in relation to online commerce via Visa, Mastercard and American Express card schemes. Furthermore, it was considered that Belgian online merchants need to migrate to new protocols allowing for full use of the exceptions to SCA. Only a small number of Belgian issuers face compliance issues in relation to the use of authentication methods for payment cards that are not SCA-compliant (first concern listed above).

Based on this analysis, on 28 August 2019, the Bank leveraged the supervisory flexibility option provided by the EBA setting out its expectations regarding market implementation – in the framework of online commerce – of the SCA procedure through the issuance of a Prudential Announcement aimed at all Belgian issuers of payment cards and Belgian acquirers of card transactions made in the framework of online commerce. The Bank referenced the aforementioned EBA Opinion, reiterated that the legal deadline of 14 September 2019 for the entry into force of SCA remained in place but acknowledged the challenges for the Belgian card payment industry in meeting this deadline and the need to work together with the relevant stakeholders (payment services providers, card schemes, merchants and consumers associations) and to agree on a reasonable and acceptable plan to migrate – as soon as reasonably possible after 14 September 2019 – for the industry to implement SCA for card payments in online commerce.



The Bank worked closely with the Belgian card payment industry to agree as soon as possible on a reasonable migration plan that encompasses a blueprint for compliance and readiness, a timetable for achieving this, and key milestones and targets to deliver improved security of customer authentication and fraud reduction along the way. In the first half of 2020, the roadmap for this migration was further finalised at Belgian level between the involved stakeholders and was published on the Bank's website in early May 2020¹. The objective of this migration plan is twofold: i) defining a realistic and feasible migration plan within the applicable deadline and ii) setting milestones to ensure a seamless and secure payment experience for merchants and consumers after the migration period.

The Bank clarified to the market that it expects all stakeholders covered by the migration plan, and in particular relevant PSPs, to fully comply with it and meet the agreed milestones and targets in order to be compliant with the SCA requirements by the final delivery date to be set out in the plan. In order to benefit from this plan, PSPs will have to provide the Bank with sufficient evidence that they have taken appropriate steps to comply with the SCA requirements at the final delivery date set out in the plan.

The Bank deliberately chose not to issue an end date for this migration as it was of the opinion this should be set at pan-European level. Accordingly, on 16 October 2019, the EBA published an Opinion on the deadline for the migration to SCA for e-commerce card-based payment transactions, effectively aimed at harmonising the deadline for supervisory flexibility by CAs in order to avoid divergent end dates for compliance with the SCA requirements. Given the intensively cross-border nature of online commerce in Europe, especially in Belgium, as well as the cross-border nature of acquiring services, it is of vital importance to ensure a common end date for supervisory flexibility. The EBA established this end date at 31 December 2020 and the Bank adheres to it.

Following publication of the Prudential Announcement, the Bank has both attended and hosted Belgian card payment industry meetings in order to help guide the birth of a reasonable and acceptable migration plan with concrete and verifiable milestones for all relevant PSPs towards full compliance with the requirements of SCA.

It should also be noted that SCA is required not only for card payment authentication but whenever payers (i) access their payment account online; (ii) initiate an electronic payment transaction (irrespective of the underlying payment instrument), or (iii) carry out any action through a remote channel which may imply a risk of payment fraud or other abuses. The Bank is therefore also tasked with monitoring compliance with the SCA requirements by all PSPs concerned since 14 September 2019, including in the online banking environment.

(ii) Open banking: access to payment accounts

A second key part of the RTS on SCA & CSC sets out common and secure communication standards (CSC) for communication between account servicing payment service providers (ASPSPs) and payment initiation and account information service providers (collectively referred to as third-party providers or TPPs). These requirements detail how ASPSPs should provide access to their payment accounts to TPPs in a secured fashion.

¹ Available at https://www.nbb.be/doc/cp/eng/2020/belgian_roadmap_sca.pdf.



The RTS on SCA & CSC provides two avenues for ASPSPs towards establishing access for TPPs to their online available payment accounts: (i) establishment of a dedicated interface; or (ii) use of an adapted customer interface. The choice between dedicated or adapted customer interface is to be made by each ASPSP. In Belgium, almost all ASPSPs have opted for the use of a dedicated interface.

When an ASPSP opts for a dedicated interface, it must provide a contingency mechanism in case its dedicated interface fails. However, provided the dedicated interface meets four requirements listed in the RTS on SCA & CSC, an ASPSP can be exempted by its CA from the requirement to foresee a contingency mechanism.

On 4 December 2018, the EBA further specified these four requirements into nine guidelines through its "Guidelines on the conditions to benefit from an exemption from the contingency mechanism under Article 33(6) of Regulation (EU) 2018/389 (RTS on SCA & CSC)". The Bank transposed these Guidelines on 19 March 2019 into its supervisory practice through issuing its Circular Letter 2019_04, at the same time detailing the application process for Belgian ASPSPs to obtain such an exemption from the Bank.

During the summer of 2019, the Bank received 18 applications for exemption from the contingency mechanism from Belgian credit institutions, one from a Belgian payment institution and one from a Belgian institution for electronic money. Twelve applications were granted before the entry into force of the RTS on SCA & CSC on 14 September 2019. Several more applications have been accepted since then.

The establishment of fully functional dedicated interfaces by Belgian ASPSPs has not been without effort. For credit institutions that provide multiple payment services (e.g. single SCT, batch payments, standing orders, future-dated payments, instant payments, etc.) across multiple online channels (mobile and website) and multiple customer segments (retail, corporate, SME, etc.), the roll-out of a set of APIs that together constitute the dedicated interface providing access to TPPs to all these payment functionalities for all payment accounts of all customers is a technically complex and lengthy process that did not end abruptly in September 2019 but will rather incrementally continue as new versions of the dedicated interface are brought into production.

Throughout 2019, the Bank engaged proactively with Belgian ASPSPs in order to clarify the relevant legal framework and its interpretation. Since the entry into force of these requirements, the Bank has been monitoring compliance by ASPSPs and TPPs and will continue facilitating dialogue between them where concerns may arise.

On 4 June 2020, the EBA published an Opinion on the obstacles to the provision of TPPs under the RTS on SCA and CSC. The Opinion aims to support the objectives of PSD2 of enabling customers to use new and innovative payment services offered by TPPs by addressing a number of issues regarding the interfaces provided by ASPSPs to TPPs. It clarifies a number of obstacles identified in the market, including requiring multiple SCAs, the manual entry of the IBAN in the ASPSPs' domain, or imposing additional checks on the consent given by the customer to the TPP. In a follow-up Communication, the Bank confirmed that it shares the stated view of the EBA and will integrate the Opinion into its supervisory approach. The Bank nonetheless acknowledged in its statement that implementation of the required technical changes to the interfaces takes time. In view of this, the Bank confirmed that it expects the sector to comply with this Opinion by 31 December 2020 at the latest.



Use of alternative techniques to access payment accounts

In the course of 2019, alternative techniques to access payment and other accounts held with Belgian ASPSPs made their entry into the Belgian market on a wider scale. This points to the rising popularity and adoption of business models seeking value in account information (and aggregation) – even beyond the scope of PSD2 – and payment initiation services.

These alternative techniques can be split into two categories: (i) screen scraping of online banking websites and (ii) reverse engineering of the mobile banking channel. In relation to the scope of PSD2, the RTS on SCA & CSC clearly sets out the communication standards between ASPSPs and TPPs. The Bank has been closely examining the detailed workings of both techniques, with a strong focus on the second one given its rising use in the Belgian market.

The Bank is convinced that a comprehensive answer to the use of alternative techniques both within and beyond the scope of PSD2 should be formulated and has been raising awareness about these issues at EU level accordingly. In this vein, the EBA clarified in its Q&A tool relating to PSD2 that ASPSPs should allow TPPs, as part of the contingency mechanism in Article 33(4) of the Delegated Regulation, to use all interfaces made available by the ASPSP to its payment service users (PSUs) for accessing their payment accounts online directly. This includes not only the ASPSP's internet banking interface, but also the ASPSP's mobile banking application made available by the ASPSP to its PSUs, where applicable. The latter does not however imply that TPPs have an automatic right to access the ASPSP's proprietary mobile banking interface that connects the ASPSP's mobile banking app to the ASPSPs' backend systems. It is the ASPSP's responsibility to ensure that TPPs can be identified and can rely on the authentication procedures provided by the ASPSP to its PSUs, in accordance with the requirements of PSD2 and the Delegated Regulation.

Furthermore, the EBA confirmed that TPPs accessing the PSUs' payment accounts using the contingency mechanism in Article 33(4) of the Delegated Regulation should also comply with their respective obligations under Article 33(5) of the Delegated Regulation, as well as with any other applicable EU legislation. In particular, access by TPPs via the PSU interface(s) should not be used as a way of circumventing the application of strong customer authentication by the ASPSP.

Supervisory Priorities in 2020

The Bank's main supervisory activities in 2020 will primarily consist of i) authorisation of new payment institutions and electronic money institutions and ii) monitoring implementation of the requirements related to the RTS on strong customer authentication and common and secure communication within the Belgian market.

With regard to the first activity, the Bank expects a further uptake of firms, both start-ups and incumbents, wishing to apply for the required authorisation to be able to provide payment initiation and account information services. Within this context, the Bank furthermore observes the following trends with regards to the business models of new service providers:

- specialised payment service providers targeting the payment activities of small and medium-sized enterprises (SMEs);
- specialised payment service providers aiming to automate, optimise and enrich payment data processing; and
- a changing offer of the incumbent banking sector to also provide new services by taking up a role of third-party provider and to access accounts of their competitors.

Regarding the first trend, the Bank has observed that a growing number of non-bank payment service providers, i.e. payment institutions and electronic money institutions, are trying to develop a competitive and personalised payment service for SMEs. New service providers argue that this is mainly driven by the fact that SMEs often require specific, individual payment solutions, which have only to a limited extent been provided by the market up to now.

The second observed trend relates to the increased data centricity in the service offering of non-bank payment service providers. Most observed business models revolve around the aggregation of account balances and the provision of digitally tailored and targeted financial services for SMEs, such as financial planning, budgeting and management. In this context, several actors are also focusing on automation of certain business processes, such as those related to cash flow management and accounting, in which account information is integrated.

In parallel to the emergence of these new market actors, existing incumbents are also focusing on integrating these new services, i.e. account information and payment initiation, into their existing product offering. The expectation for 2020 is therefore that more Belgian banks will launch the possibility to consult payment accounts held with other Belgian banks in their own channels as well as to initiate payment orders from that other payment account.

With regard to the second foreseen activity of the Bank in 2020, that of monitoring of the implementation of the requirements related to the RTS on strong customer authentication and common and secure communication, specific focus will be laid on both the migration plan for SCA in online commerce with payment cards and the roll-out of dedicated interfaces in Belgium, which would foster the full deployment of payment initiation and account information services within the market (for more details, see box 9).

For SCA, the focus will be on ensuring that the migration plan is followed by all domestic market participants. The Bank will at the same time continue its ongoing monitoring of SCA compliance across all payment service providers in the market.

For access to payment accounts, the focus will be on actively monitoring developments taking place within this context and ensuring the creation of stable and fully functional dedicated interfaces enabling the provision of TPP services in the Belgian market. Furthermore, the Bank will continue its work in relation to the use of alternative techniques for accessing payment and other accounts.

The continued transformation of the payments market, combined with further developments related to *open banking*, will show whether new service providers can develop a sustainable business model and obtain a permanent and stable stake within the payments landscape. The Bank will therefore actively monitor developments taking place within this context.

Money remittance in Belgium

In 2019, two online money remittance companies were granted a licence by the Bank. In total, seven money remittance companies were listed as Belgian payment institutions at the end of 2019. Belgian payment institutions have an agent network of 244 agents in Belgium and 7 998 agents¹ in other EEA countries. In addition to the 244 Belgian agents, 1 657 agents from other European payments institutions are active in Belgium.

At the end of 2018, the total amount of incoming and outgoing money transfers via money remitters was € 1 319.9 million. Belgian payment institutions accounted for € 356.9 million, or 27.04 % against € 962.9 million of all EU money remitters active in Belgium.

Taking into account both incoming (IN) and outgoing (OUT) money transfer flows, Morocco (22 %), Turkey (10 %) and Romania (9 %) are still the major countries for the money remittance business taking place in Belgium in value terms (chart, left-hand panel). By number of transactions, Morocco (24 %), the Democratic Republic of Congo (12 %) and Romania (8 %) account for the largest share (chart, right-hand panel).

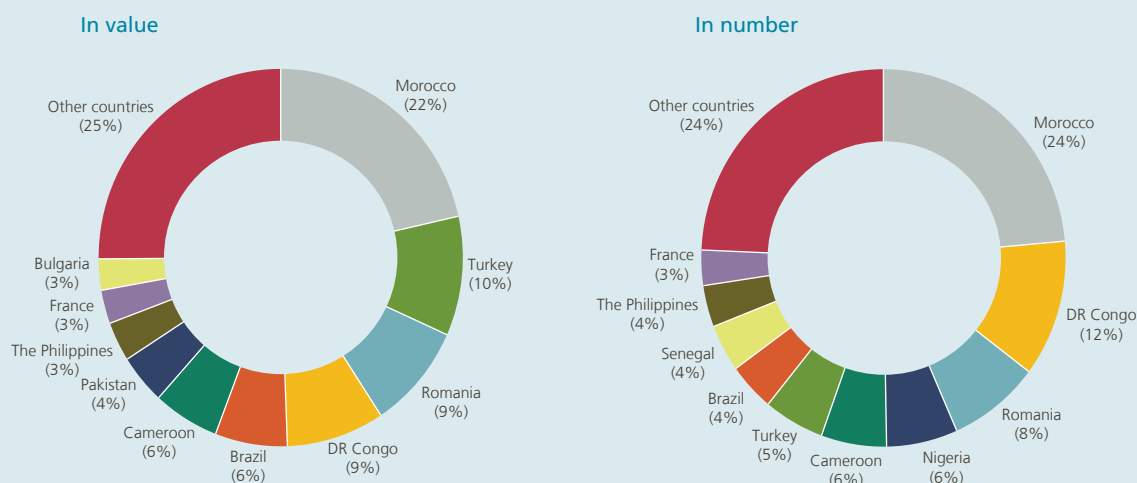
¹ 92 % of the agents work in name and behalf of Moneygram International, which re-located from the UK to Belgium at the end of 2018 due to Brexit.

Overview of money remittance in Belgium

Money transfers by all money remitters present in Belgium

(2018, yearly total, payment institutions established in BE or other EEA Member States, IN & OUT money transfer flows)

Chart – Top-10 Country Corridors



3.3 Processors of payment transactions

Changes in regulatory framework

There were no changes in the Belgian regulatory framework in the course of the period running from April 2019 to April 2020.

Prudential and oversight approach

In 2019, one legal entity which is providing processing services in the Belgian payments market was designated as a systemically important payment processor. In line with Article 6 of the Law of 24 March 2017 on the oversight of payment transactions processors, the NBB's Board of Directors has designated Mastercard Europe as a systemically important processor of payment transactions performed through its card payment scheme (CPS) Maestro based on the data collected for the year 2018 from Mastercard Europe as a CPS.

Processors which qualify as being of systemic importance have to meet a specific set of requirements that aim to maintain the stability and continuity of retail payments in Belgium. One example of these requirements relates to the obligation for having a comprehensive risk management in the fields of detection, appraisal and development of mitigation measures. The legal framework on payment transaction processors also consists of a strict process for incident reporting to the Bank and the ability for the latter to apply a sanctions regime.

Supervisory priorities in 2020

The Bank will keep its focus on cyber resilience of systemically important payment processors and continue to monitor the evolution in that respect. As a part of its monitoring activities, the Bank carried out an on-site "IT security inspection" on Worldline in 2019. Implementation of the action plan designed to answer the recommendations issued by the Bank will be monitored in 2020. (For Mastercard, see the next section on card payment schemes.)

3.4 Card payment schemes

Regulatory framework

The regulatory framework devoted to card payment schemes remained unchanged over the period running from April 2019 to April 2020.

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, is in charge of the standard-setting process with regard to the oversight framework, as well as the planning of assessments to be undertaken in all jurisdictions. For domestic CPSs, the compliance assessment is, as a general 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 any assessment of its compliance with the Eurosystem CPS standards are peer reviewed at the Eurosystem level.

For international CPSSs, the process is similar except that (i) the assessment work is shared among the members of the assessment group made up of representatives of the NCBs having a legitimate interest in overseeing the international CPS, the coordination of which is 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 (MCE), established in Belgium, and for which the Bank ensures the role of overseer within the Eurosystem framework coordinating the assessment group.

During the 2019 classification exercise of payment systems, the Eurosystem concluded that MCE ought to be listed as a systemically important payment system¹ (SIPS), due to its important payments clearing function. This additional qualification² requires MCE to comply with the requirements of the SIPS Regulation (including the CPMI-IOSCO PFMI referred to above) and the Cyber Resilience Oversight Expectations for FMIs (CROE), which define the Eurosystem's expectations in terms of cyber resilience.

The CROE are based on the guidance on cyber resilience for FMIs, which was published by the CPMI-IOSCO in June 2016. The Cyber Resilience Oversight Expectations themselves aim to provide overseers with a clear framework to assess the cyber resilience of systems and 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 eight specific domains³ which of the three maturity levels (Evolving, Advancing, Innovating) must be achieved by the systems according to their risk profiles and specific activities.

In addition to the above-mentioned frameworks, the Regulation on interchange fees for card-based payment transactions (IFR) requirement on the unbundling of scheme and processing activities within the same legal entity also applies to MCE and Visa Europe. The designated national competent authorities of eight Member States in charge of enforcing the unbundling requirement for MCE and Visa Europe have agreed that the Bank (for MCE) and the UK Payment Systems Regulator (PSR, having supervisory competence for Visa Europe established in London) would set up a cooperative mechanism for monitoring compliance with IFR Art. 7.1.a. The Bank was formally designated by seven other NCAs as lead NCA in charge of coordinating the cooperative working group devoted to MCE. In its capacity as NCA for MCE, the Bank has been duly informed by MCE about the effective measures put in place to comply with this Regulation.

Based on a detailed questionnaire commonly agreed upon in the cooperative working group, the Bank has (a) collected from MCE its answers in substance and underlying evidence, and (b) started to assess compliance with those implemented measures.

Oversight priorities in 2020

Stemming from the designation of MCE as a SIPS, particular focus is put on assessing its compliance with the SIPS Regulation (encompassing the PFMI requirements) and the CROE requirements. These assessments will be performed in coordination with an assessment group, consisting of participating Eurosystem NCBs, and under the joint lead oversight of the Bank and the ECB.

Regarding the IFR cooperation mechanism for ensuring compliance of MCE with IFR Art. 7.1 a, the assessment exercise, performed by the whole cooperative working group, is expected to be finalised at the 2020 Q4 / 2021 Q1 horizon.

The compliance of Bancontact with article 7.1 of the IFR will be reviewed in the course of 2020. Bancontact is fully compliant with the current oversight standards. This assessment will be reviewed in case of significant evolution of the scheme or if the applicable Eurosystem oversight framework is updated.

¹ <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020XB0026&from=EN>.

² Mastercard remains a CPS, the additional qualification as SIPS only covers clearing and settlement function of the CPS.

³ The eight domains covered by the CROE are Governance, Identification, Protection, Detection, Response and Recovery, Testing, Situational awareness and Learning and evolving.

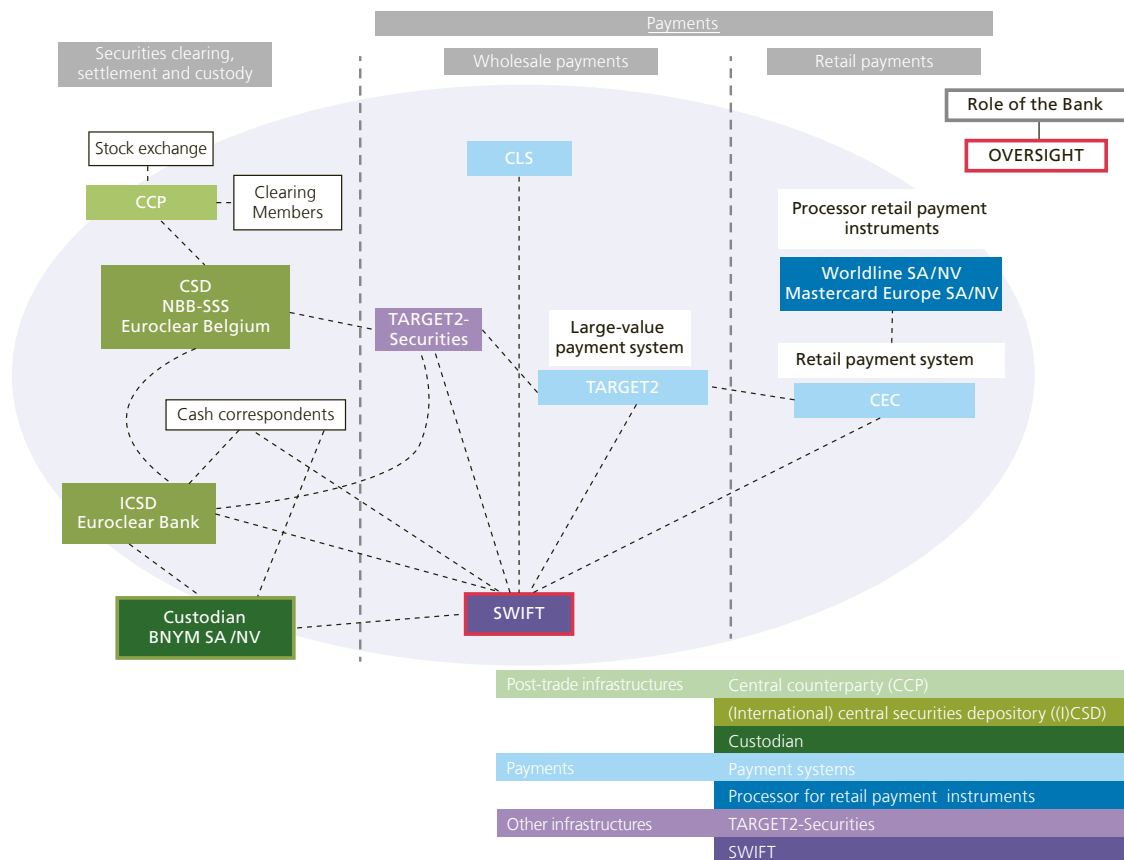
4. SWIFT

The Society for Worldwide Interbank Financial Telecommunication (SWIFT) is a limited liability cooperative company registered in Belgium. SWIFT provides messaging and connectivity services to a wide variety of financial institutions and market infrastructures, including banks, brokers, investment managers, fund administrators, trading institutions, treasury counterparts and trusts.

SWIFT is a critical service provider to systemically important correspondent banking activities and financial market infrastructures (see chart 5). Therefore, the G10 central banks have identified SWIFT as systemically important.

Chart 5

SWIFT as a critical service provider to the financial industry



4.1 Oversight approach

An international cooperative arrangement has been established to oversee the safe and efficient functioning of SWIFT. As SWIFT is based in Belgium, the National Bank of Belgium has been appointed as lead overseer.

BOX 11

International dimension of SWIFT

SWIFT operates in an international context by having activities in more than 200 countries. In 2019, 8.4 billion FIN messages (+7.4 % compared to 2018) were sent, with a daily average of 33.5 million messages.

SWIFT's users own the company and interact with the Board and Executive Committee through national member groups¹, user groups² and dedicated workgroups. Shares are allocated based on message traffic over the SWIFT network. Every three years, there is a redistribution of the shares to realistically reflect changes in the use of SWIFT messaging. Countries or country constituencies appoint directors to the SWIFT Board based on the number of shares owned by all users in the country. The next redistribution is planned to take place in the first quarter of 2021. On top of the discussions with its national member groups and user groups, there is ongoing dialogue with industry specific workgroups. The topics for discussion touch upon various domains: revision of standards, service changes, new technology implementations, security enhancements.

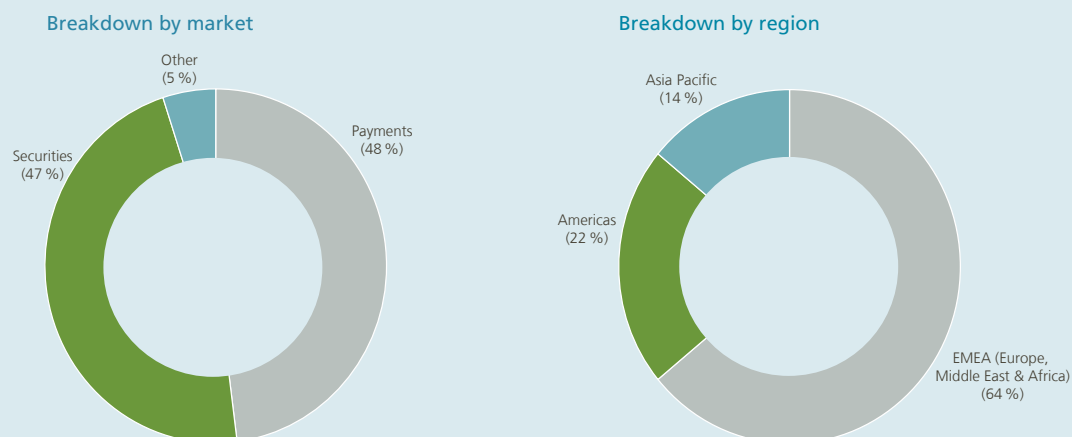
The following two charts give an overview of the 2019 SWIFT FIN activity per market and region. FIN is SWIFT's core messaging service for exchanging financial messages. There are over 11 000 live users of whom 2 420 represent shareholders. Last year, the lion's share of FIN traffic is distributed between payments (48 %) and securities (47 %) messaging. The Europe, Middle East and Africa (EMEA) region took the largest part (64 %) of the total 2019 FIN traffic flow.

1 The national member group is represented by all SWIFT shareholders within the same country. It excludes subsidiaries and branches of foreign financial institutions or corporates. The national member groups are involved in the consultation of product evolutions and technology developments.

2 The national user groups are made up of SWIFT users from the same country. These groups discuss operational themes (e.g. migrations, standard releases, local trainings, technical implementations affecting users in the country). The national user groups are also involved in the discussions about product developments and technology changes.



SWIFT FIN activity



International cooperative arrangement

The international cooperative arrangement for the oversight of SWIFT sets out a framework for oversight by the National Bank of Belgium and the central banks of the G10/G20 jurisdictions.

As lead overseer, the NBB conducts the day-to-day follow-up of SWIFT activities and coordinates the different working groups:

The **Cooperative Oversight Group** (OG) consists of the 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) and the chairperson of the CPMI. The OG discusses oversight policy and strategy. Two OG meetings take place every year.

The **Executive Group** (EG) is a sub-group where direct talks with SWIFT's Board and Executive Management are held on the central banks' oversight policy, issues of concern, SWIFT's strategy regarding oversight objectives, and conclusions. The EG represents the OG in discussions with SWIFT and can pass on OG recommendations to SWIFT. The EG members are Bank of Japan, Federal Reserve Board, Bank of England, European Central Bank and National Bank of Belgium, and meet three times a year.

The **G10 Technical Group** (TG) does the technical fieldwork on important developments within SWIFT and reports back to the OG. Since the TG performs deeper technical analysis, there are four meetings planned each year. At every TG meeting, there is a direct interaction with SWIFT management, internal audit and independent risk functions in order to carry out the technical groundwork for oversight. Skills and

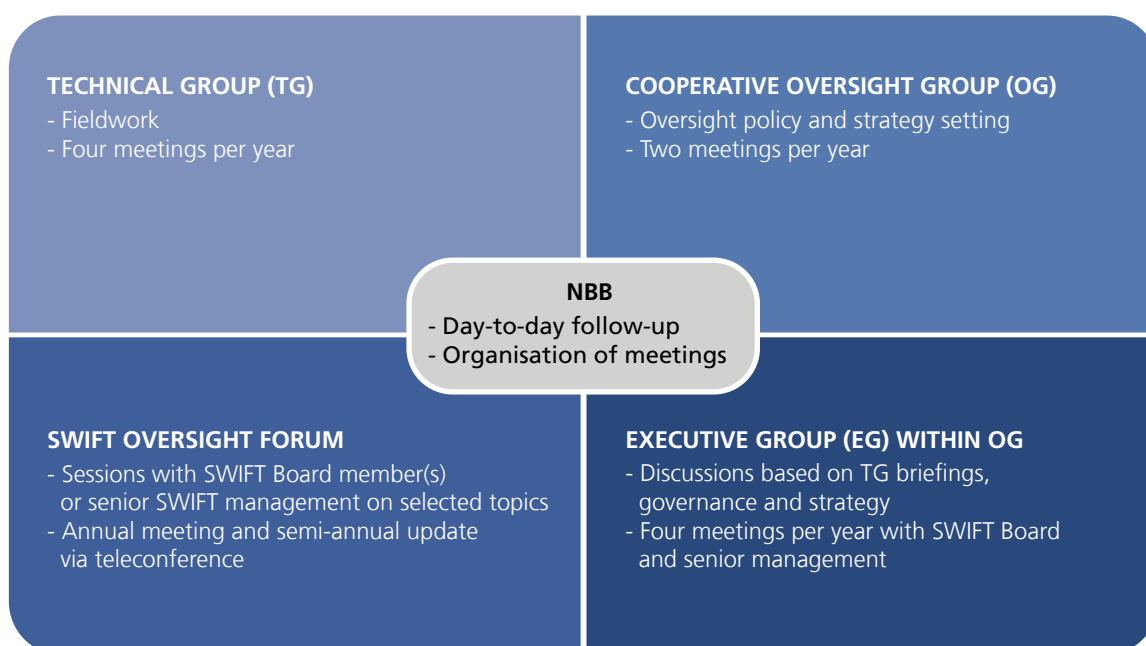
knowledge on technological and IT-specific domains are necessary to better understand these developments and their accompanying risks within SWIFT.

The **SWIFT Oversight Forum (SOF)** involves a larger group of countries, who represent a significant part of the SWIFT traffic volume. This working group consists of 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). Their membership is aligned with the composition of the CPML. In 2019, five additional central banks joined the SOF: Central Bank of the Argentine Republic, Banco Central do Brazil, Bank of Indonesia, Bank of Mexico and Banca de España. The SOF holds discussions on oversight policy, provides input for OG priorities, and serves as a platform for communication on system interdependencies related to the common use of SWIFT. The NBB is continuously seeking ways of improving its outreach to other central banks, as indicated in box 12.

The chart below gives an overview of the different working groups involved in the SWIFT oversight.

Chart 6

Cooperative oversight of SWIFT



Outreach activities

In 2018, the IMF recommended the Bank to further extend its information-sharing efforts, which resulted in a series of outreach activities.

The NBB organised its second outreach session at SWIFT's yearly Sibos conference in 2019 in London. More than 70 participants from over 50 countries joined this second session. The advantages of organising the outreach session at SIBOS are threefold: (i) a large delegation of central banks attend the conference, (ii) each time the conference is located in a different continent, (iii) central bank representatives and directors of the payments, IT and FMI oversight departments predominantly attend Sibos.

Oversight expectations

Overseers' core expectations are rooted in five high-level expectations (HLEs): (i) Risk Identification and Management, (ii) Information Security, (iii) Reliability and Resilience, (iv) Technology Planning, and (v) Communication with users¹.

The five HLEs focus on the adequate management of operational and technology risks. SWIFT oversight is structured around the HLEs for its risk-based activities planning, discussions and decisions to take. The five expectations evolved into generic oversight requirements for all critical service providers to FMIs and are formalised in Annex F of the CPMI-IOSCO Principles for FMIs. Overseers expect SWIFT to report back on its compliance with the HLEs. This reporting serves as input for oversight analysis and provides an overview of the risk drivers for SWIFT. As such, enterprise risk management, information security and technology risk management are part of the standing oversight activities covered by the HLEs.

A multitude of approaches with varying intensity and duration are at the overseers' disposal. Box 13 discusses the oversight tools that complement overseers' recurrent analyses on the effectiveness of SWIFT's implementation of the five HLEs.

¹ For more detailed information, see FMI Report 2017 or CPMI-IOSCO Principles for FMIs – Annex F: Oversight expectations applicable to critical service providers.

Tools for the oversight of SWIFT

Every TG meeting includes a full day where overseers have a direct interaction with SWIFT management, and second and third lines of defence. SWIFT is invited to update the overseers on developments, incidents, risk reviews, technological changes and projects impacting the entire SWIFT stature.

Senior SWIFT representatives are frequently invited to present their views and directions at OG and SOF meetings. And representatives of SWIFT's Board and Executive Committee attend EG meetings to discuss a variety of topics.

The TG meetings at SWIFT are a snapshot of what is going on in the company and provide overseers with rich information for their work. However, certain developments and changes that are of considerable importance require continuous oversight (e.g. endpoint incident analysis and audit reviews). On top of the four regular TG meetings, ad-hoc meetings with TG members are held whenever necessary to discuss certain topics.

In addition to the technical meeting with SWIFT, overseers have also initiated another oversight tool to gain a better grasp of certain topics and their operations. The already existing interactions with SWIFT give an opportunity to gain broader knowledge. To gain more profound knowledge, deep-dive sessions have been launched. These sessions are designed to gain detailed insight into certain areas, departments, functions, interactions at SWIFT and include the three lines of defence. The deep-dive sessions are arranged at a TG meeting on top of the traditional full-day meeting at SWIFT. Overseers' decision to hold a deep-dive session depends on the consensus reflecting any lack of clear understanding of a certain domain. For example, overseers invite the project owner to explain a major project and its implications on the entire company. So far, overseers have held two deep-dive sessions to obtain deeper knowledge in certain areas.

Another oversight tool that overseers apply at their discretion is the on-site review. The first on-site review kicked off at the end of 2018 and was finalised in 2019. In light of the HLEs, overseers scope a certain area they wish to distinguish so as to look into more closely. Whereas the deep-dive session consists of a half-day discussion on a certain topic, the on-site review is a more dedicated way of understanding a domain and its functioning. Over an entire week, meetings between overseers and different SWIFT representatives are planned. Findings and recommendations are passed on to SWIFT. Accordingly, a follow-up plan is established for which SWIFT is expected to comply with overseers' expectations. Overseers select on-site review topics that are not traditionally fully covered by previous TG oversight tools. An illustration of the objective of the first on-site review was to get a transparent end-to-end overview of the enterprise risk management process.

The SWIFT Customer Security Programme and related fraud detection and prevention tools received considerable attention from overseers in 2019. Also, projects like the ISO20022 migration for cross-border payments traffic have come under overseers' review.

4.2 Covered oversight topics in 2019

Overseers' activities are mainly concentrated around cyber and technological topics. They seek to obtain assurance that the corresponding risks in these domains are adequately assessed, monitored and mitigated in spite of the reliability of the services. Topics like the Customer Security Programme, decisions impacting the IT infrastructure and standing interactions with the three lines of defence were included in the 2019 oversight work.

Customer security programme (CSP)

SWIFT's Customer Security Programme (CSP) aims to strengthen the security of the global financial community against cyber threats by providing requirements for users in terms of how they should secure their own local IT infrastructure used for connecting to SWIFT. In 2019, overseers devoted a considerable amount of time to reviewing the effectiveness of the CSP.

The Customer Security Control Framework (CSCF) has been analysed by overseers on the effectiveness of the implementation and reporting processes. The CSCF is a set of mandatory and advisory controls applicable to every SWIFT user. Mandatory security controls establish a security baseline with which all SWIFT users must comply, whereas advisory controls describe good practices for securing local IT infrastructures. All SWIFT users were required to self-assess their compliance with the CSCF and upload this information through SWIFT's KYC-Self Assessment (KYC-SA) tool by the end of 2019. Overseers observed an uptake in the number of self-attestations in 2019; by 31 December 2019, 91 % of customers, representing 99 % of SWIFT's payments traffic, had attested their level of compliance with the mandatory security controls. Overseers actively follow up on the CSP quality assurance metrics provided by SWIFT. These metrics give an overview of the attestation, consultation, reporting processes' effectiveness, and the security advances across different user types. Quality assurance metrics are continuously being refined and extended by the overseers to improve their monitoring activities.

SWIFT performs an annual review of the CSCF, which overseers review in turn. Other stakeholders are involved in the review process as well, like cyber security experts, supervisory authorities and SWIFT users. Aligned with best practices, two advisory controls were promoted to mandatory and two new advisory controls were added to the most recently updated CSCF version. Multiple existing controls received clarifications on their implementation.

The implementation design of the enhanced KYC-SA supervisory role has been under examination, too. In 2019, the overseers also considered which information supervisors need to perform their activities effectively. SWIFT reserves the right to report users who have failed to timely self-attest full compliance with all mandatory CSCF controls or who depend on non-compliant service providers (i.e. service bureau or shared infrastructure provider) to the competent supervisory authorities. The self-attestation information could be an important input for risk-based planning and scoping for supervisory authorities. Previously, supervisors received information on self-attestation status of BICs in their jurisdiction via SWIFT Post (information push). SWIFT plans to overhaul this process by implementing a supervisory role in the self-attestation tool (information pull).

Overseers reviewed SWIFT's independent assessment framework and will continue to follow-up on the framework's effectiveness over the course of 2020. As of mid-2021, all SWIFT users are required to substantiate their self-attestations with an independent assessment conducted by internal or external auditors. The assessments must cover all applicable mandatory controls specified in the latest version of the CSCF.

Users have the possibility to consult information in their counterparties' CSCF self-attestations to obtain insight into their security position and take appropriate risk-mitigation measures. There has been an increase in counterparty consultations by a varied group of SWIFT users. Overseers will continue to monitor this consultation process. SWIFT's getting started guide for assessing cyber security counterparty risk has also been assessed by overseers.

In 2019, overseers assessed the design and implementation of the recently introduced Payment Control Service (PCS), and existing fraud prevention and detection tools. In addition to the security specifications SWIFT users must comply with, the CSP also sets out how a user can prevent and detect fraud in commercial relationships. SWIFT offers various tools to prevent and detect fraud incidents. The PCS is an example of such a tool. It is an optional tool that aims to help SWIFT users combat fraudulent payments and strengthen their existing security measures.

SWIFT's communication channels to inform its users on technology changes, to interact with compromised users in crisis situations, and to update users on fraud practices of adversaries have been analysed by overseers on their effectiveness and rigour. The CSP also includes how information-sharing in the wider community helps a user to adequately organise incident and risk management processes from any future cyber threats. SWIFT's Information Sharing and Analysis Centre (ISAC) portal contains a large and digestible amount of information targeted to both technical and business professionals on new cyber threats, indicators of compromise, tools and techniques used by hackers.

It is in overseers' interest to obtain reasonable assurance on the effectiveness of the evolving security requirements for users to reduce the risks for SWIFT, its users and the entire community. An important oversight objective is to ensure that these security requirements continue to evolve in line with emerging threats, advances in cyber security practices and regulatory developments.

Other topics

Besides the review of the CSP in the context of financial stability for the wider ecosystem, the core focus remains on the security and availability of SWIFT's critical messaging services.

Cyber security is a top priority for the overseers. Over the course of 2019, overseers continued to focus on the design, implementation and testing of cyber-event detection, response and recovery measures. SWIFT's roadmap setting out its cyber security strategy, improvements and plans has been evaluated and assessed against the strong-changing threat landscape. Furthermore, the impact of new technologies and processes on SWIFT's risk profile have also been closely followed up by overseers. Additionally, overseers have been paying attention to other types of risk than technical ones (e.g. business, third-party risks), namely the recurrent assessment of extreme risks and recovery plans.

Overseers conduct frequent reviews of the effectiveness of the various lines of defence and governance structures for daily operations, long-term strategies and specific projects. In 2019, they challenged these internal and external actors on their opinions, findings and further planned control work. In practice, there have been frequent interactions with SWIFT's Chief Auditor, Chief Risk Officer, and one yearly meeting with the external security auditor. The in-depth review of the enterprise risk management framework kicked off in 2018 and was finalised last year. This review gave better insight into the level of design, integration and implementation of the framework. The first in-depth review has been evaluated as successful and will be a recurrent exercise for the oversight of SWIFT.

Overseers also reviewed how SWIFT applied its cyber security requirements to third-party providers of interface products and shared infrastructure providers. Users can opt to connect to SWIFT through a third party instead of installing the interface products on their premises. Overseers closely followed up on the

security strategy that SWIFT applied to ensure all parties that connect to its network were in accordance with SWIFT's security specifications.

Incidents, like disruptions of SWIFT's services, are closely investigated by overseers. The sequence of events, user impact and results of the outcome of the investigations are analysed. Overseers are informed about the incident and the completeness and adequacy of the corresponding action plans. These action plans are frequently followed up in order to prevent recurrence of similar incidents. The incidents are discussed with SWIFT and further research is carried out if required.

SWIFT's long-term strategy and how it is aligned with specific infrastructure investment often comes under discussion between overseers and SWIFT's management and Board. Overseers typically challenge the security and strategic focus of such plans. For example, they reviewed SWIFT's ISO 20022 migration plan and will follow up on its further progress in 2020 and 2021, and implementation in 2022. Also, the design and roll-out plans of the new interface offering Alliance Cloud have been and will be on the agenda for review.

4.3 Oversight priorities in 2020

The planning of oversight activities results from a risk-based analysis, which is rooted in the five HLEs.

Given the evolving cyberthreat landscape, the focus remains on the adequacy of SWIFT's cyber strategy. More specifically, overseers review the multi-year cyber security roadmap update and progress, which aims at protecting SWIFT's infrastructure, networks and operations. The work of the external security auditor is closely analysed and challenged by overseers.

Overseers will continue to dedicate their support and devoted attention to the CSP. The importance of maintaining the CSCF control framework and monitoring thereof will remain in overseers' standing focus of activities. Relevant metrics to monitor the effectiveness of the Programme will be maintained. Furthermore, overseers continue to engage the refinement of existing and request of additional metrics. As in previous years, 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 outreach to the different stakeholders. Special attention will be paid to the proposed enhancements of the self-attestations (i.e. independent assessment framework, counterparty consultation, information pull for supervisory authorities).

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

First of all and in line with our mission, overseers continuously monitor the effectiveness of the three lines of defence (i.e. SWIFT's management, independent risk management function and internal audit function). More specifically, overseers review the management's risk identification and assessments, as well as the effectiveness of the mitigating measures. The development and implementation of the entire ERM methodology and risk acceptance processes are periodically reviewed by overseers. Furthermore, internal and external audit reports are under continuous analysis where overseers follow up on the audit findings and mitigations actions management undertakes.

Secondly, the initiatives that SWIFT undertakes to improve its business continuity management framework and disaster recovery strategies, with respect to the requirements of the CPMI-IOSCO guidance on cyber resilience, are planned for review. More specifically, the focus will be on how SWIFT recurrently assesses

its extreme cyber risk scenarios and its progress towards the achievement of the two-hour recovery time objective (2h-RTO). Referring to the HLEs for information security and technology planning, overseers expect SWIFT to continuously identify gaps and make improvements for their cyber security strategy. The maturity of SWIFT's cyber practices is also planned for continuous review.

Thirdly, overseers will continue assessing the adequacy of processes for monitoring changes in technology risk for the existing infrastructure in place and the maturity of technology performance, scalability, and security for technology choices considering SWIFT's future infrastructure. Confidentiality, integrity and availability are three conditions that are envisaged during overseers' assessment. Recurring topics of attention are SWIFT's third-party vulnerability management and incident response processes.

Fourthly, the initiatives SWIFT is taking to improve communication processes for informing its users will be examined. These involve keeping clients informed about new interface releases (i.e. interface hardening Alliance 7.4 in 2020), updates on new malicious events (e.g. SWIFT ISAC report on new phishing e-mails), interacting with users in crisis situations (e.g. updating incident response guidelines), and engaging in new major developments (e.g. ISO 20022 migration for cross-border payments).

Finally, the overseers will closely analyse the presented design and follow-up of the implementation of major projects and developments that could have a significant impact on SWIFT's critical services and overall risk stature. Discussions with the involved SWIFT representatives of the three lines of defence and breakdown of the relevant documentations are standing practices herein.

COVID-19 impact on SWIFT and oversight activities

As many other international organisations, SWIFT has had to adapt and react to the impact of the pandemic outbreak. Given SWIFT's presence and activities in every continent, it has been monitoring the situation in a timely manner and in accordance with national and local authorities' measures.

As a critical service provider to the financial sector, SWIFT has focused on keeping its critical infrastructure operational to avoid any interruption of global financial messaging traffic. Despite the physical closure of its offices, business continuity has been ensured by promoting working from home for all employees. SWIFT has continuously assessed its staff organisation so that the key staff at the necessary SWIFT locations have been able to work. SWIFT has also reduced the burden on its customers by taking a series of additional mitigating actions, like the one-year delay of new features of its annual standards release.

Most governments have taken measures to limit the economic damage by launching national lockdowns. The global economic slowdown has resulted in an impact on SWIFT messaging. The effects of these measures could be clearly observed in the first half of 2020 (from January until June). Payments traffic grew by 2.1 %, whereas this growth was 4.9 % during the same period last year. In 2019, payments traffic grew by 5.5 %. Securities and treasury traffic grew compared to the same period last year as result of the volatility in the market. Securities posted a growth of 21.7 %, whereas in 2019 this was 8.3 %. In 2019, total securities traffic grew by 9.1 %. Also, treasury traffic showed a similar trend; posting 25.0 % growth in June 2020 compared to 9.4 % in June 2019. Despite the lower payments traffic together with the higher growth of securities and treasury traffic, overall FIN traffic growth was 12.1 %, which was almost double compared to the first semester of 2019 with a growth of 6.6 %.

Overseers adapted their activities to the crisis situation. However, they continued their critical review on SWIFT in areas such as cyber, Enterprise Risk Management, CSP, Internal Audit topics, with in addition COVID-19 implications on the various topics under review. Traditionally, there are multiple physical meetings with different central banks throughout the year. The governmental restrictions such as closed borders and physical distance demanded a decentralised approach to conduct the planned oversight work. Teleconference meetings replaced the physical meetings as the alternative to ensure that the appropriate analysis on SWIFT could be continued. On top of the standing SWIFT oversight meetings, outreach activities also had to be rearranged in another format. In general, the pandemic has not blurred the oversight priorities and overseers continue to profoundly assess SWIFT's activities from a cyber- and operational-risk-based view.

Thematic article:

Emerging practices for pandemic resilience

Filip Caron

Since the outbreak of SARS-CoV-2 in late 2019, financial market infrastructures (FMIs) have increasingly faced adverse effects as the infectious disease outbreak rapidly gained pandemic proportions. Both the industry and authorities have been focusing on the appropriate management of risks related to resource (people, processes, technology, facilities and information) failure.

Existing business continuity plans and working-from-home (WFH) arrangements have been successfully leveraged to guarantee operational resilience in the short term. However, a pandemic may further complicate an operator's ability to respond to additional operational stress events.

Pandemic recovery plans that enable FMIs to continue providing robust platforms and operations consider challenges that deviate from those encountered in more stereotypical business continuity scenarios. Unlike incidents caused by natural disasters, infrastructure failures or cyber attacks, the pandemic scenario needs to consider prolonged and potentially recurring periods of widespread operational stress as a pandemic is not a one-off incident impacting a specific location.

Belgian FMIs, payment systems and critical service providers have continued to provide reliable services to their participants and customers during the first wave of the pandemic. This article aims to identify both best and emerging pandemic resilience practices, but also looks beyond coping with the direct impact of the pandemic.

Emerging practices for immediate response

Over the course of January 2020, the risk of a widespread and potentially global pandemic became increasingly real. As a result, major FMIs started putting the initial stages of their pandemic recovery plans into practice.

A pandemic recovery plan typically defines which sets of risk-mitigating measures need to be employed in different pandemic phases (e.g. interpandemic phase, alert phase, pandemic phase and transition phase as defined by the World Health Organisation). As the global average of cases increases – as well as the direct impact for the infrastructure, system or service provider defined in terms of absenteeism or number of infections – executive and steering committees decide to gradually roll out the pandemic recovery plan and implement risk-mitigating measures.

Ensuring the availability of employees critical to core operations and service provisioning has been a top concern for continuity and recovery planning. There are several reasons for wider unavailability of key employees, including sickness, issues with remote work arrangements, individual challenges like childcare and mental health concerns.

Additionally, FMs need to comply with the pandemic guidelines issued by the domestic and local authorities. As lockdowns became the norm in most jurisdictions around the globe, these guidelines mandated extensive WFH arrangements with limited exceptions for critical workers.

Emerging and best practices *for the initial pandemic phases*, typically characterised by greater vigilance as the virus has been identified in humans and an epidemic develops in at least one remote jurisdiction :

- **Establishing an appropriate governance team:** Managing implementation of the pandemic recovery plan should be the responsibility of a steering committee composed of executives and key experts. Additionally, separate task forces may be established to address specific business continuity, technical, legal, human resources, communication and health related challenges;
- **Guaranteeing staff safety:** Ensuring the welfare and safety of employees should be the top priority. Education and awareness campaigns are a natural starting point for raising staff safety and reducing the likelihood of infection. Office health supplies including hand sanitisers and personal protection equipment like face masks and gloves should be acquired and distributed. FMs should aim at reducing staff interaction by avoiding large meetings and extending working hours to reduce crowding in their facilities. Employees who return from countries or regions badly affected by coronavirus or become ill should self-isolate. Furthermore, FMs should review visitor procedures and restrict business travel;
- **Acknowledging critical services and roles:** Identifying services (e.g. settlement processes) that must be guaranteed throughout the pandemic, as well as the roles needed to provide these services. Scenario analysis based on varying impact on absenteeism provides better insight in the adverse effect and additional mitigating actions. Examples of these additional mitigating actions include explicitly defining redundant teams for critical roles and identifying individuals that could be rapidly cross-trained when needed. The latter requires up-to-date and readily-available procedures, manuals and handbooks;
- **Preparing for WFH arrangements:** Assessing the ability to timely activate long-term and large-scale remote working. FMs should review existing WFH arrangements for critical employees; test the capacity and scalability of IT infrastructure (including authentication mechanisms) supporting the WFH arrangements; and review the control framework to ensure effective and secure WFH arrangements;
- **Reviewing incident response processes:** Evaluating different incident scenarios to determine the ability to timely and effectively respond to (operational) incidents. FMs should plan adequately for scenarios that could not be managed remotely. This includes ensuring that additional staff can physically enter the FMs' facilities, offering safe and timely transport options and minimising the likelihood of infection on the premises;
- **Reviewing succession plans:** Establishing the processes and triggers to delegate authority when senior managers and executives become unavailable. Clear upfront communication should reduce the potential risk of disorientation.

Additional measures taken *as the number of infections rapidly increases and a pandemic outbreak becomes reality* include:

- **Enacting WFH arrangements:** Activating long-term and large-scale WFH arrangements, while ensuring that critical workers obtain permits – in line with authorities' guidelines – to access the technical infrastructure if needed;
- **Monitoring the physical and mental health of employees:** Tracking sickness and unavailability among employees, which will guide the implementation of additional measures of the recovery plan. Furthermore, isolation and extreme stress due to increasing responsibilities at work or at home may result in declining motivation or even burn-out among staff members. Therefore, human resource management should focus

on identifying early signs of deteriorating mental health and proactively provide tools to further minimise unavailability of key employees.

Preparing for continued and additional operational stress

Since the first quarter of 2020, Belgian FMIs and their participants have been operating under exceptional circumstances. However, it is important for FMIs to maintain adequate operational resilience as stipulated in the CPMI-IOSCO's Principles for Financial Market Infrastructures and Guidelines on Cyber Resilience, under these rapidly evolving non-business-as-usual circumstances.

Additional operational stress events may result from physical infrastructure failures, cyber and information security incidents and payment and settlement delays. A massive switch to WFH arrangements has stimulated the creativity of cyber attackers in developing COVID-19-related attack vectors (e.g. specific phishing campaigns), while the number of endpoints may have increased significantly. Moreover, as control frameworks might have been revised to support WFH arrangements (e.g. missing physical access controls and secure document disposal), these endpoints may be more attractive for cyber attackers.

Some FMIs have been confronted with unprecedented transaction volumes. Transaction volumes observed at these FMIs at the beginning of the European lockdowns required an upscaling of the capacity of information systems. In a limited number of cases, settlement and risk management processes have been impacted and operating hours needed to be extended.

Authorities have requested FMIs and other incumbents of the financial services industry to critically review their business continuity plans (including the pandemic recovery plan) in light of the current operational environment. FMIs' executives and senior managers are responsible for designing and updating their pandemic recovery plan, as well as translating the plan into concrete policies, processes and procedures. Boards of directors are responsible for overseeing the establishment and evolution of the pandemic recovery plan, as well as reviewing the related resource investment and testing.

But an FMI's response to an additional operational stress event may not only depend on its own ability to handle incidents, both remotely as on premises. FMIs may depend heavily on critical service providers as well as IT infrastructure and technology solution providers. The status of critical infrastructure which SWIFT has obtained in all jurisdictions critical to its messaging service provisioning grants crucial exemption in times of lockdown (e.g. a limited number of critical staff are allowed to travel and access critical facilities). Not obtaining critical infrastructure status may significantly impact the IT infrastructure and technology solution providers' ability to respond in a timely manner to an operational incident and could have knock-on effects on FMIs' operational resilience.

The following emerging and best practices in updating business continuity and pandemic recovery plans have been observed:

- **Identifying and interacting with critical third parties:** Obtaining in-depth insight into the business continuity provisions of critical providers is crucial for determining the ability to guarantee critical service provisioning during the pandemic. Furthermore, whenever an FMI cannot gain reasonable assurance on the adequacy or effectiveness of service providers' plans, it should prepare contingency plans for shifting to alternate providers;
- **Re-evaluating the pandemic extreme risk scenario:** Assessing the extent to which business continuity plans address the pandemic extreme scenario, as well as the ability to implement, scale and sustain additional

measures in good time. For example, traditional business continuity plans typically leverage alternate sites to deal with natural disasters or other emergencies. However, during pandemics, FMI may be faced with shortages of available staff to relocate and – as is currently observed with the COVID-19 pandemic – the alternate sites may be severely impacted as well;

- **Finetuning the metrics and triggers of the pandemic recovery plan:** Developing detailed monitoring systems to more accurately capture the progression of viral outbreaks and specify triggering events. In addition to traditional news sources, a variety of alternative yet highly reliable sources have emerged during the COVID-19 pandemic, e.g. the detailed and integrated statistics provided as well as the critical trend analyses by Johns Hopkins University. These additional data points should enable more detailed implementation of mitigating measures, as well as a closely controlled return to business as usual, although a business-as-usual scenario may only be achieved after a vaccine has been found;
- **Re-assessing the cyber threat level and controls:** Identifying emerging weakness due to increasing security backlogs or relaxed controls to enable WFH arrangements, as well as evolving cyber threat landscapes as attackers take advantage of general disorientation and confusion (e.g. in phishing mails). FMI could enhance monitoring capabilities for their critical information systems which act as (partially) compensating controls to timely detect a cyber attack. Furthermore, FMI should continue raising awareness of cyber security risks. Similarly, there have been indications of increased targeting of participants' operated endpoints.

The COVID-19 pandemic has resulted in extended periods of uncertainty and operational stress, potentially impacting available critical resources and other project inputs like stakeholder interaction. FMI may face significant project delivery risks and may need to reprioritise projects. Embarking on numerous new projects in combination with significant pre-COVID-19 technology renewal may result in excessive demands on critical resources and derail strategic responses to market developments.

Emerging practices include:

- **Assessing impact of the pandemic on project delivery:** Identifying the potential impact of a pandemic on the availability of supporting resources and processes (including training and dependency management). Reviewing the demands on key resources to enhance security and efficiency for WFH arrangements, including demands related to legal and regulatory requirements;
- **Coordinating with key stakeholders:** Reviewing the capacity of stakeholders both internal and external to contribute to key projects, e.g. ability to review prototypes and engage with agile software development teams or availability for resilience testing. FMI have also allowed their participants additional time to meet less critical requirements;
- **Assessing risks induced by the pandemic and formulate risk responses:** Establishing appropriate risk identification and assessment processes to review proposed delays and request formal risk acceptance by management where needed. The Board of Directors' risk committees are responsible for the oversight of these risk management practices.

Planning for the resumption of onsite working

At the end of the second quarter of 2020, the average daily number of new cases fell sharply in Europe, as the transition phase of the pandemic was entered. FMI started considering reopening facilities for non-critical staff in a gradual and cautious manner.

The resumption of onsite working involves a series of precautionary measures, as the threat of a second and subsequent waves remains realistic:

- **Gauging the comfort level of employees:** Engaging with employees to understand their willingness and ability to return to the office. Several important challenges have been identified in this context, notably related to commuting (because employees are keen to avoid public transport) or to a lack of appropriate childcare. Most FMs anticipated that WFH would remain standard practice for most employees, at least until the end of the third quarter of 2020. As a result, FMs continue to invest in productivity training for remote collaboration;
- **Phasing in the return to onsite working:** Working with split teams to ensure back-up for critical functions. Establish work schemes that alternate onsite working and WFH. Reallocate employees across different sites to mitigate undue risks in any one location. FMs may also start analysing requests to restart non-critical services that require physical presence and identify the employees supporting these functions.
- **Ensuring physical workspace safety:** Deep cleaning and implementing other infection control measures for physical facilities. Redesign foot traffic flows to avoid congestion and enable appropriate social distancing. Establish symptom monitoring controls like temperature checks, which although not fully watertight may identify potentially infected employees. Ban large meetings with personal attendance. Continue pandemic awareness campaigns;
- **Redesigning of processes and workflows:** Reducing the number of physical handovers to the absolute minimum and automate critical processes wherever possible.

Actions by authorities

Belgian supervisors and overseers of FMs, payment systems and critical service providers have been reviewing the appropriateness of the pandemic recovery plans and continue to closely monitor any adjustments made in the light of the evolving pandemic risk.

Special attention is being placed on obtaining reasonable assurance on the effectiveness of the different lines of defence during the pandemic. Supervisors and overseers continue to monitor and challenge the appropriateness of risk-mitigating measures, including measures related to the scalability of IT infrastructure, to the ability to respond to incidents and to the improvement of cyber resilience.

The Bank is represented in the CPMI and actively contributes to analyses of the effectiveness of WFH arrangements and operational resilience in times of a pandemic.

Annexes

Annex 1: Regulatory framework

FMI s	<p>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)</p> <p>http://www.bis.org/cpmi/publ/d101a.pdf</p>
	<p>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.</p> <p>http://www.bis.org/cpmi/publ/d106.pdf</p>
	<p>CPMI-IOSCO Recovery of financial market infrastructures (October 2014): Guidance for FMIs and authorities on the development of comprehensive and effective recovery plans.</p> <p>http://www.bis.org/cpmi/publ/d121.pdf</p>
	<p>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.</p> <p>http://www.bis.org/cpmi/publ/d146.pdf</p>
	<p>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.</p> <p>https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf</p>
CCP s	<p>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.</p> <p>http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012R0648&from=EN</p>

CCPs	<p>EMIR Refit: Regulation (EU) 2019/834 of 20 May 2019: mainly simplifies the derivatives' reporting and clearing obligation requirements, but also imposes CCPs to provide information on their initial margin models, including simulation tools, to their clearing members. Further, the European Commission gets the power to suspend the clearing obligation for selected derivatives contracts e.g. where markets become disrupted.</p> <p>https://eur-lex.europa.eu/eli/reg/2019/834/oj</p>
	<p>EMIR 2.2: Regulation (EU) 2019/2099 of 23 October 2019: it improves consistency of supervisory arrangements for CCPs established in the EU, and enhances the EU's ability to monitor, identify and mitigate third-country CCP risks.</p> <p>https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R2099</p>
	<p>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.</p> <p>http://www.bis.org/cpmi/publ/d125.pdf</p>
	<p>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.</p> <p>http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R2205&from=EN</p>
	<p>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.</p> <p>https://www.bis.org/cpmi/publ/d163.pdf</p>
CSDs	<p>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.</p> <p>http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0909&from=en</p>
	<p>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</p> <p>http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0389&from=EN</p>
	<p>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</p> <p>https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0390&from=EN</p>
	<p>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</p> <p>http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0392&from=EN</p>

Custodians	<p>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.</p> <p>https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0391&from=EN</p>
	<p>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.</p> <p>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</p>
	<p>ESMA Guidelines on Internalised Settlement Reporting under Article 9 of CSDR (March 2018)</p> <p>https://www.esma.europa.eu/press-news/esma-news/esma-finalises-guidelines-how-report-internalised-settlement</p>
Payment Systems	<p>ECB Regulation (EU) No 795/2014 on oversight requirements for systemically important payment systems (July 2014): Regulation, based on the CPMI-IOSCO PFMLs, covering systemically important payment systems in the eurozone, large-value and retail payment systems.</p> <p>https://www.ecb.europa.eu/ecb/legal/pdf/oj_jol_2014_217_r_0006_en_txt.pdf</p>
	<p>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.</p> <p>https://www.ecb.europa.eu/pub/pdf/other/revisedoversightframeworkretailpaymentsystems201602.en.pdf?bc332d9a718f5336b68bb904a68d29b0</p>
PIs & ELMIs	<p>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.</p> <p>http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0110&from=EN</p>
	<p>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.</p> <p>http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015L2366</p>
	<p>Belgian Law of 11 March 2018 transposing the PSD2, Belgian Official Gazette 26 March 2018.</p> <p>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</p>

Payment Processors	<p>Belgian Law of 24 March 2017 on supervision of payment transactions processors, <i>Belgian Official Gazette</i> 24 April 2017. https://www.nbb.be/doc/cp/moniteur/2017/20170424_opp_wet_loi.pdf</p>
	<p>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. (FR) or (NL)</p>
Card Payment Schemes	<p>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/oversightfcardpaymentsss200801en.pdf</p>
	<p>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</p>
	<p>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</p>
	<p>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): <i>Belgian Official Gazette</i> 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</p>
	<p>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</p>

SWIFT	<p>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.</p> <p>https://www.nbb.be/en/financial-oversight/oversight/critical-service-providers#oversight-of-swift-</p>
	<p>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.</p> <p>http://www.bis.org/cpmi/publ/d101a.pdf</p>
	<p>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.</p> <p>http://www.bis.org/cpmi/publ/d123.pdf</p>

Annex 2: FMIs established in Belgium with an international dimension

Euroclear

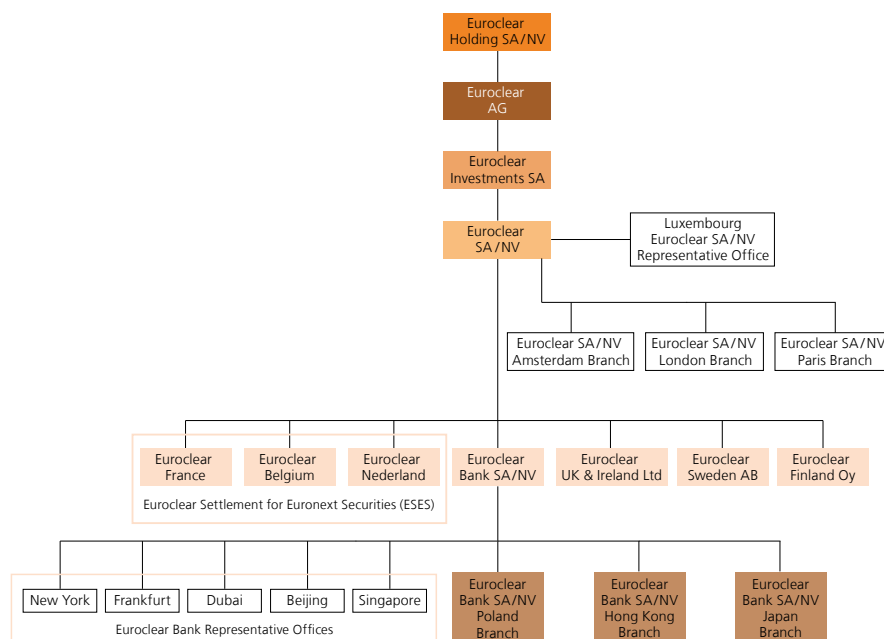
Euroclear Holding SA/NV, the top financial holding of Euroclear, is incorporated under Belgian law. Euroclear Holding SA/NV owns 100 % of Euroclear AG, a Swiss financial holding company. Euroclear Investments SA is the group's financial investment holding company, incorporated in Luxembourg.

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 Nederland, Euroclear Belgium), Euroclear UK & Ireland Ltd, Euroclear Sweden AB, Euroclear Finland Oy and Euroclear Bank SA/NV. The latter has branches in Poland, Hong Kong and Japan. Euroclear Group (I)CSDs have outsourced the IT production and development to ESA. ESA also delivers common services, such as risk management, internal audit, and legal and human resources services to the Group (I)CSDs.

Chart 1

Euroclear Group Corporate Structure

(simplified diagram)

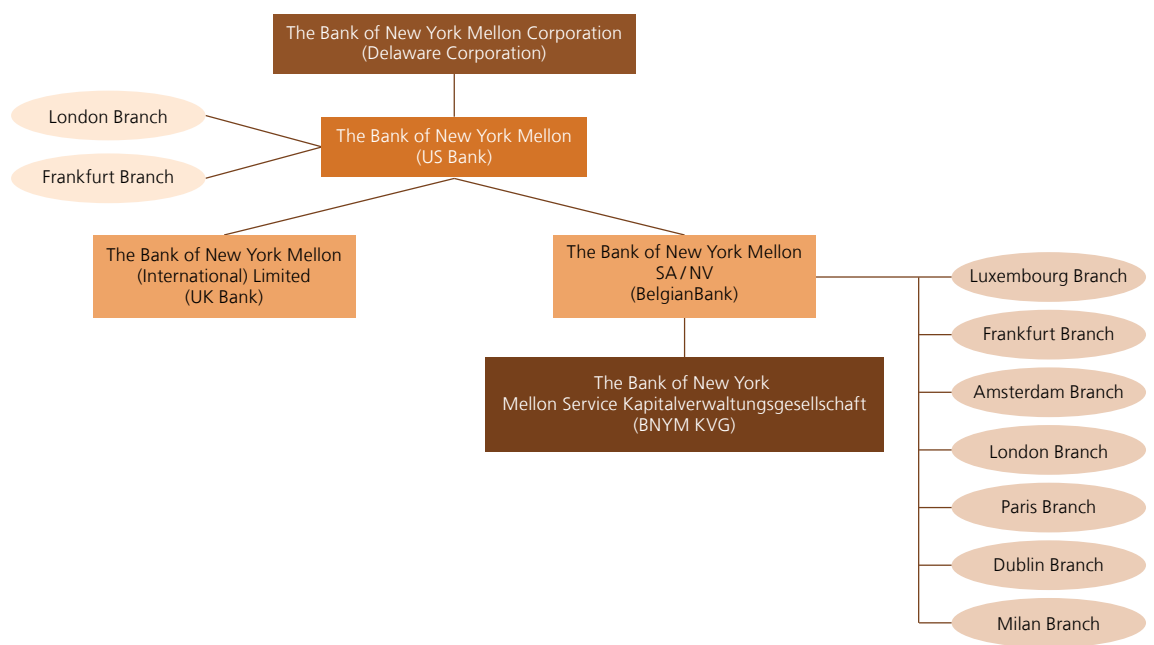


Source: Euroclear.

The Bank of New York Mellon

The Bank of New York Mellon SA/NV (BNYM SA/NV), established in Belgium, is the European subsidiary of BNY Mellon, a US based global systemic bank, which in turn is a subsidiary of the US holding company BNY Mellon Corporation. BNYM SA/NV is the custodian of the group for European clients and its European gateway to the euro area markets and payment infrastructures. BNYM SA/NV has a 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).

Chart 2
BNYM Group structure and BNYM SA/NV position
(simplified diagram)



Source: NBB.

Worldline

Worldline is a French group providing electronic payment and transactional services in Europe and beyond. It used to be a division and full subsidiary of the European IT services corporation Atos. Since 2014 Worldline SA (France) is listed on Euronext Paris.

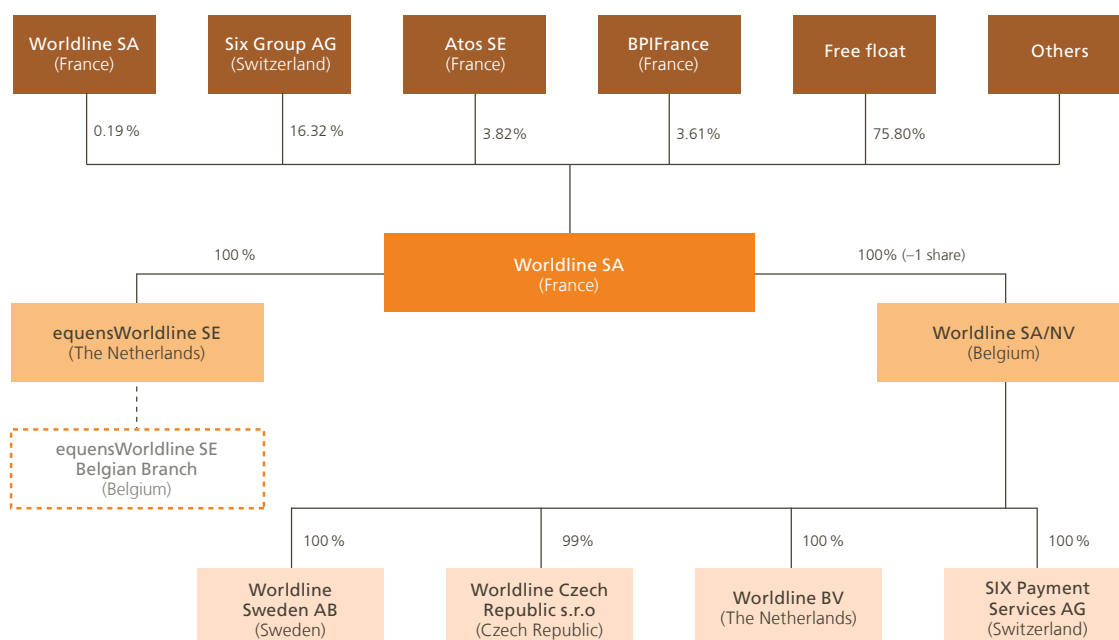
In 2016, Worldline SA/NV, the Belgian entity of the group merged with the Dutch company Equens. The processing activities were carved out in a new entity called equensWorldline SE. equensWorldline SE is now a full subsidiary of Worldline SA (France).

In 2018, Worldline acquired Six Payment Services, the payment division of the Swiss company SIX, which is now the main shareholders of Worldline SA (France) with more than 16.32 % of the shares. Since 2019 more than 75 % of Worldline's outstanding shares are owned by public investors (free float). With the acquisition of Ingenico announced in February 2020, Worldline will become the largest European provider of payment services.

Chart 3

Structure of Worldline

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



This scheme presents a simplification of the Worldline Group focusing on the entities which are relevant in the context of this report.

Source: Worldline.

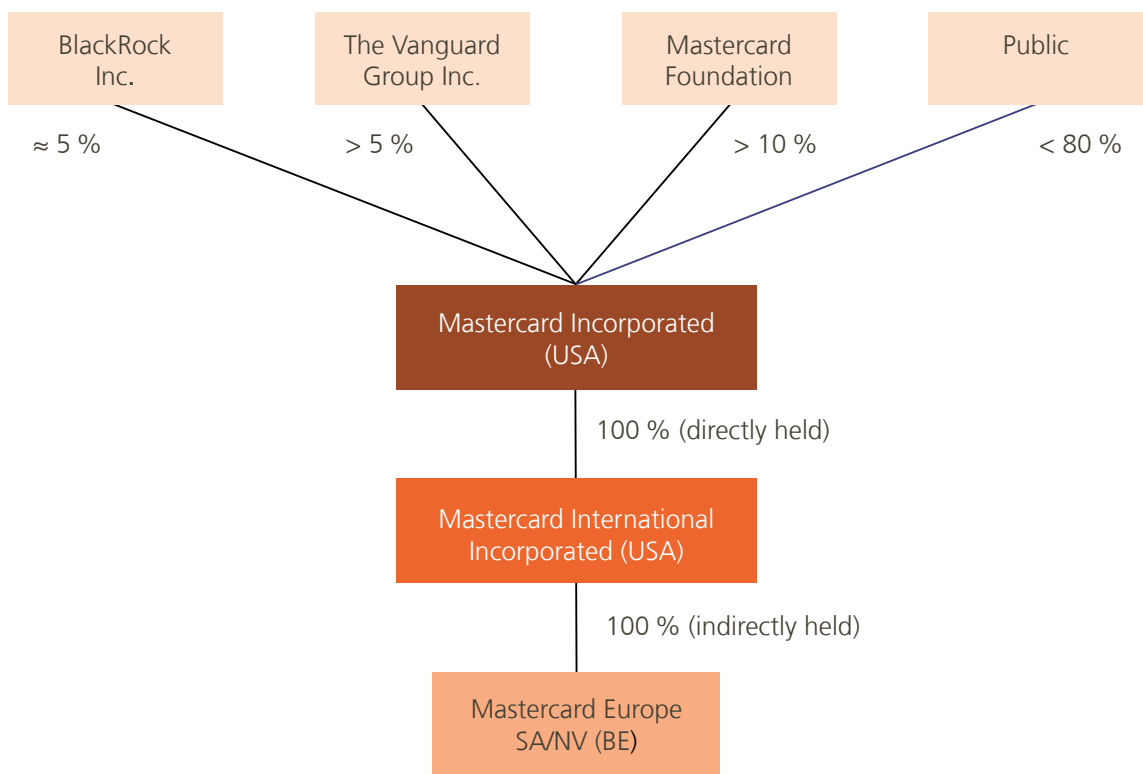
Mastercard Europe

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.

Chart 4

Mastercard Group Structure

(simplified diagram, as of January 2020)



Source: NBB.

Annex 3: Statistics

List of tables

<i>Tables relating to Securities Clearing, Settlement and Custody</i>	85
A. Central Counterparties (CCPs) (selected)	85
B. Euroclear Bank	86
C. NBB-SSS	86
D. Euroclear Belgium	86
E. TARGET2-Securities	86
F. BNYM SA/NV	86
 <i>Tables relating to Payments</i>	 87
A. TARGET2	87
B. CLS Bank	87
C. Centre for Exchange and Clearing (CEC)	87
D. Payment institutions (PIs) – Electronic Money Institutions (ELMIs)	88
E. Processors of payment transactions (Worldline SA/NV)	88
F. Card transactions	89
G. Card schemes (Bancontact)	89
 <i>Table relating to SWIFT</i>	 90

Table 1

Securities Clearing, Settlement and Custody

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

	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
A. Central Counterparties (CCPs) (selected)										
LCH Ltd (UK)										
Repos (all currencies combined)	118 322	93 331	84 108	79 245	78 118	79 300	77 039	87 553	89 822	
LCH SA (FR)										
Credit Default Swaps (all currencies combined)	56	62	91	336	123	346	898	1 098	1 225	
Repos (Belgium, all currencies combined)	842	701	985	1 341	1 567	1 345	1 259	890	1 128	
Eurex Clearing AG (DE)										
Repos (all currencies combined)	12 870	20 210	16 838	20 858	28 953	22 251	12 084	9 025	11 299	
Source: ECB Central Counterparty Clearing Statistics.										

Table 1 (continued)

Securities Clearing, Settlement and Custody

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

	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
B. Euroclear Bank										
Value of securities deposits (end of period)	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	14 823.6
Number of transactions (in millions)	47.7	59.4	64.2	69.5	75.2	83.3	84.1	95.4	107.0	116.4
Value of transactions	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	544 564.8
Source : Euroclear.										
C. NBB-SSS										
Value of securities deposits (end of period)	494.0	513.3	531.2	541.7	557.3	575.4	612.5	625.3	632.6	646.65
Number of transactions (in millions)	0.4	0.5	0.6	0.6	0.6	0.5	0.5	0.5	0.5	0.5
Value of transactions ¹	9 049.6	14 133.9	10 250.1	8 428.0	8 209.0	8 766.5	8 714.5	9 069.8	11 164.8	8 693.1
Source : NBB.										
1 Secondary market turnover.										
D. Euroclear Belgium										
Value of securities deposits (end of period)	162.0	130.4	156.8	202.7	222.1	269.4	235.1	237.7	178.0	220.2
Number of transactions (in millions)	1.8	1.9	1.9	1.9	2.1	2.5	2.4	2.5	2.7	2.6
Value of transactions	497.7	588.0	563.6	799.8	714.8	944.6	963.8	946.0	964.1	783.9
Source : Euroclear.										
E. TARGET2-Securities										
Number of transactions (in millions)	nap	nap	nap	nap	nap	7.6	36.3	125.6	145.9	154.8
Value of transactions	nap	nap	nap	nap	nap	43 706.8	112 066.0	192 175.0	236 050.8	282 063.7
Source : ECB. T2S was launched in 2015.										
F. BNYM SA/NV										
Value of assets held under custody (end of period)	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	2 873.5
Source : BNYM.										

Table 2

Payments

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

	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
A. TARGET2										
Value of payments	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	441 280.9
of which : TARGET2-BE	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	24 935.5
Number of payments (in millions)	87.2	89.0	89.6	91.3	87.8	88.6	89.0	89.3	88.4	87.8
of which : TARGET2-BE	2.4	2.6	2.5	2.3	2.5	2.3	2.2	2.3	2.3	2.5
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)	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	1 362 882.2
of which : EUR payments	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	249 090.1
Number of payments (in millions)	198.1	206.9	176.6	205.0	204.7	219.1	209.5	198.5	226.6	257.1
of which : EUR payments	42.2	45.5	37.4	36.9	34.4	40.9	34.3	34.0	39.1	42.2
Sources : ECB Payment Statistics, CLS.										
C. Centre for Exchange and Clearing (CEC)										
Value of payments	846.9	886.7	909.1	911.6	870.7	883.4	920.6	941.8	1 122.9	1 204.7
Number of payments (in millions)	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	1 512.7
Sources : ECB Payment Statistics, NBB.										

Table 2 (continued 1)

Payments

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

	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
D. Payment Institutions (Pis) – Electronic Money Institutions (ELMIs)										
Pis										
Belgian Pis	1	9	9	11	15	17	21	24	22	26
Foreign Pis with Belgian branch	0	0	2	2	3	3	3	2	3	4
Passport notifications for cross-border services										
Belgian Pis towards other EEA countries	11	19	19	26	41	65	162	218	248	440
Foreign EEA Pis towards Belgium	47	104	133	184	262	273	379	421	435	511
ELMIs										
Belgian ELMIs	6	6	6	10	10	10	8	8	7	7
Foreign ELMIs with Belgian branch	0	0	0	0	1	1	1	1	2	1
Passport notifications for cross-border services										
Belgian ELMIs towards other EEA countries	15	18	19	43	45	69	70	72	72	104
Foreign EEA ELMIs towards Belgium	8	14	28	40	54	53	102	156	188	240
Institutions offering services within a limited network (new under PSD2)	nav	nav	nav	nav	nav	nav	nav	nav	1	4
Transactions by Belgian Pis and ELMIs (in millions)										
Number of transactions (yearly total)	nav	nav	nav	1 665	1 874	1 968	2 155	2 006	2 044	1 949
Value of transactions in euro (yearly total)	nav	nav	nav	105 989	133 513	136 567	137 144	124 388	124 485	113 639
Average outstanding E-Money of Belgian ELMIs	nav	nav	nav	15.2	21.8	35.8	45.5	73.9	116.6	405.2
Source : NBB.										
E. Processors of payment transactions										
Worldline SA/NV										
Number of transactions (yearly total, in millions) 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	1 548	1 692
Source : Worldline.										
¹ Since 2017, as a consequence of the transfer of some processing activities to equensWorldline SE, volumes reported in this table only refer to acquiring activities of Worldline SA/NV.										

Table 2 (continued 2)

Payments

F. Card transactions	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Number of cards issued by resident payment service providers – Cards with a cash function										
Number of cards (in thousands, end of period)					21 396.54	21 875.01	22 593.13	22 016.35	23 904.69	nav
Number of cards per capita (end of period)					1.91	1.95	2.00	1.94	2.10	nav
POS transactions at terminals provided by resident PSPs										
Number of payment transactions per card – With cards issued by resident PSPs (yearly total)					49.8	49.8	55.4	80.1	73.0	nav
Value of payment transactions per card – With cards issued by resident PSPs (yearly total, in €)					2 391.7	2 697.3	2 759.1	3 829.6	3 374.5	nav
Transactions per capita										
Number of card payments – With cards issued by resident PSPs ¹ (yearly total)					135.2	131.3	150.0	170.5	183.7	nav
Value of card payments – With cards issued by resident PSPs ¹ (yearly total, in € thousands)					7.2	7.4	8.1	8.8	9.0	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)										
of which:										
Retail payments	1 076.4	1 136.4	1 180.4	1 241.8	1 306.7	1 389.5	1 441.6	1 480.2	1 593.4	
ATM	973.4	1 028.9	1 068.4	1 125.9	1 190.9	1 272.8	1 325.2	1 336.0	1 488.8	
	103.0	107.5	111.9	115.9	115.9	116.8	116.3	114.2	104.6	
Source: Bancontact.										

Table 3

SWIFT

(yearly total, in millions)

	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Number of messages	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	8 454.4
of which:										
Payment messages	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	4 053.4
Securities messages	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	3 968.9
Other messages	267.3	330.5	299.4	325.6	330.3	347.3	367.3	359.0	398.1	432.1
Source : SWIFT.										

List of abbreviations

AISP	Account information service provider
ASPSP	Account servicing payment service provider
BCBS	Basel Committee on Banking Supervision
BCP	Business Continuity Plan
BNYM	Bank of New York Mellon
BRRD	Bank Recovery and Resolution Directive
CCP	Central counterparty
CEC	Centre for Exchange and Clearing
CLS	Continuous Linked Settlement
CPMI	Committee on Payments and Market Infrastructures
CPS	Card Payment Scheme
CROE	Cyber Resilience Oversight Expectations for FMIs
CSC	Common and Secure Communication
CSDR	CSD Regulation
CSD	Central Securities Depository
CSP	Customer Security Programme
D-SIFI	Domestic systemically important financial institution
DTCC	Depository Trust & Clearing Corporation
DVP	Delivery versus payment
EBA	European Banking Authority
EC	European Commission
ECB	European Central Bank
EEA	European Economic Area
ELMI	Electronic money institution
EMD	Electronic Money Directive
EMEA	Europe, Middle East and Africa
EMIR	European Market Infrastructure Regulation
EPC	European Payments Council
ESA	Euroclear SA/NV
ESCB	European System of Central Banks
ESES	Euroclear Settlement of Euronext-zone Securities
ESMA	European Securities and Markets Authority
EU	European Union
FCA	Financial Conduct Authority
FMI	Financial market infrastructure

FSB	Financial Stability Board
FSMA	Financial Services and Markets Authority
FX	Foreign exchange
G-SIB	Global systemically important bank
G-SIFI	Global systemically important financial institution
HLE	High Level Expectation
ICSD	International central securities depository
IFR	Regulation on interchange fees for card-based payment transactions
IOSCO	International Organisation of Securities Commissions
IP	Instant Payments
ISAC	Information sharing and analysis centre
JST	Joint Supervisory Team
LSI	Less significant institution
LVPS	Large-Value Payment Systems
MCE	Mastercard Europe
MoU	Memorandum of Understanding
NCA	National competent authority
NCB	National central bank
ORPS	Other retail payment system
O-SII	Other systemically important institution
OTC	Over the counter
PFMIs	CPMI-IOSCO Principles for FMIs
PI	Payment institution
PIRPS	Prominently important retail payment system
PISP	Payment initiation service provider
POS	Point of sale
PSD	Payment Services Directive
PSP	Payment Service Provider
PSU	Payment Service User
PVP	Payment versus payment
RPS	Retail payment system
RRP	Recovery and resolution planning
RTS	Regulatory Technical Standard
SCA	Strong Customer Authentication
SCT Inst	SEPA instant credit transfer
SEPA	Single European Payments Area
SI	Systemically-relevant credit institution
SIPS	Systemically important payment system
SIRPS	Systemically important retail payment system
SSM	Single supervisory mechanism

SSS	Securities settlement system
SWIFT	Society for Worldwide Interbank Financial Telecommunication
T2	TARGET2
T2S	TARGET2-Securities
TTP	Third-party provider

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



Publisher

Tim Hermans

Executive Director

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

Contact for the publication

Johan Pissens

Deputy Director

Surveillance of financial market infrastructures, payment services
and cyber risks

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

© Illustrations: National Bank of Belgium

Cover and layout: NBB CM – Prepress & Image

Published in September 2020

Printed on FSC paper

