Financial Market Infrastructures and Payment Services

Report

2021

National Bank OF BELGIUM
Eurosystem

Financial Market Infrastructures and Payment Services

Report

2021

National Bank OF BELGIUM
Eurosystem

The Financial Market Infrastructures and Payment Services report is dedicated to Johan Pissens, former head of Surveillance of financial market infrastructures, payment services and cyber risks.

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, C. Cabaret, F. Caron, C. Collaert, D. De Beuckeleer, S. Goret, P. Gourdin, D. Gui, J. Jans, V. Olécrano, T. Plomteux, J. Rosewick, F. Saffer, H. Sefsaf, S. Siedlecki, C. Stas, R. Temmerman, J. Uytterhoeven, S. Van Cauwenberge, A. Van Genechten, I. Vansieleghem, J. Vermeulen

Contents

Executive summary

Belgium hosts a number of significant financial market infrastructures (FMIs), custodians, payment services providers, as well as critical service providers, 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 on these systems and institutions headquartered in, or relevant for, Belgium.

COVID-19

One major event that marked 2020 was of course the COVID-19 pandemic, which affected these systems and institutions in various ways. Some institutions, such as central securities depositories (CSDs) and custodians, saw increased transaction volumes thanks to the volatility in the markets, while others, such as money remitters, were negatively affected by government measures such as the lockdown in March 2020. Sometimes, the impact proved to be temporary (e.g. the market volatility in March), while other changes, such as consumer preferences for contactless payments or online shopping, are expected to be more permanent.

Most FMIs, payment service providers and critical service providers were well prepared to deal with extreme scenarios and had business continuity arrangements in place such as large-scale home working for staff. The coronavirus crisis did lead to an increased number of COVID-19 themed cyber attacks overall, leading to an increased vigilance by FMIs.

During the pandemic, authorities adapted their way of working (e.g. working from home, virtual meetings) and continued their oversight and supervision tasks. One notable exception was the third regional SWIFT oversight outreach session, which was planned during the physical 2020 Sibos conference, which was converted into a digital Sibos, which made it impractical to organise the foreseen oversight outreach session.

Brexit

Brexit was another major event that received the authorities' attention. The Bank has assessed the readiness of global custodian BNY Mellon SA/NV with regard to Brexit and the compatibility of the business model set-up with a post-Brexit environment. EU CSDs, payment institutions and electronic money institutions that wish to continue to provide services in the UK, will need to apply for a UK licence. Similarly, UK institutions that wish to continue to operate in the EU, will need an EU licence. Since 2017, seven UK payment/electronic money institutions have been relocated to Belgium, which underlines the importance of Belgium as a location for these institutions. In March 2021, Irish securities have migrated to the Belgian international CSD Euroclear Bank from the UK CSD Euroclear UK & Ireland.

Despite the COVID-19 pandemic and Brexit, the regular oversight and supervision activities have continued in order to address short-term priorities as well as to work on longer-term projects to improve financial stability.

Regulatory initiatives

On the regulatory front, international regulators have issued new guidance with regard to recovery and resolution of central counterparties (CCPs). The EU regulatory framework for CCPs has also been updated (and called EMIR 2.2) in 2020. That year, a targeted review of the EU regulatory framework for CSDs (CSDR) was launched. In response to recent trends, the European Commission has taken two are regulatory initiatives that may affect various categories of institutions : the Digital Operational Resilience Act (DORA) and the Regulation on Markets in Crypto Assets (MiCA). The emergence of crypto-currencies (incl. stablecoins) has prompted the central banks of the Eurozone to start investigate a central bank digital currency (CBDC). These topics are further discussed in thematic articles in this Report.

Oversight and supervision activities

In addition to monitoring the impact of the COVID-19 pandemic and the related government measures – which highlighted the importance of operational resilience – and Brexit, the Bank has continued its regular oversight and supervision activities.

Cyber security remains one of the main attention points. 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 included monitoring progress of adherence with and raising awareness about the cyber controls of the CSCF and assisting in the promotion of the framework with bank supervisors. The Bank also monitored implementation of the CSCF by institutions under its oversight work in 2020. In addition to the CSCF, the SWIFT overseers also followed up the planned ISO 20022 migration for cross-border payments and cash management among others.

In order to further enhance the cyber resilience of Belgian critical institutions, the Bank implemented the Threat Intelligence Based Ethical Red teaming (TIBER) framework developed by the ECB in Belgium under the name TIBER-BE, on which a thematic article has been dedicated in this Report.

In the field of payments, the Bank monitored the implementation of the strong customer authentication (relevant for the growing e-commerce activities) and secure communication standards (open banking) requirements. Furthermore, the Bank, as lead authority for the card payment scheme Mastercard Europe, has completed an analysis of Mastercard Europe's compliance with the Regulation on interchange fees for card-based payment transactions requirement on the unbundling of scheme and processing activities within the same legal entity.

Finally, in 2020, the Bank as national competent authority has conducted its first annual review and evaluation under the CSDR of Euroclear Belgium, which was authorised in 2019 under the CSDR. The NBB-SSS is operated by the central bank and therefore legally not subject to an annual review and evaluation by the national competent authority. Nevertheless, as the NBB-SSS is eligible for Eurosystem credit operations, the Eurosystem has assessed the NBB-SSS against the CSDR requirements which are relevant from a user perspective (as the Eurosystem is a user of the CSD). Oversight also monitored implementation of the NBB-SSS project to offer delivery-versus-payment (DVP) transactions in foreign currencies, which removes the so-called settlement risk. This is the risk linked to non-DVP transactions, whereby sellers of securities transfer their securities before receiving the cash payment. When the buyer defaults before paying, the sellers lose the entire value of the securities that they transferred. For buyers that pay before they receive the securities, the same settlement risk exists. By linking the exchanges of securities and cash together, the NBB-SSS has eliminated this risk for cash in foreign currencies – for euros this was already the case.

The review and evaluation under the CSDR of Euroclear Bank, which was authorised under the CSDR at the end of 2019, has been initiated at the end of 2020.

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.

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.

FMIs and financial institutions that provide securities clearing, settlement and custody services are considered part of the post-trade securities landscape. The clearing of a trade via a central counterparty (CCP) generally means that the CCP becomes the buyer counterparty for the seller and the seller counterparty for the buyer.

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

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

Financial institutions that facilitate their clients' access to securities investment markets are referred to as custodians. In that capacity of intermediary, custodians can offer their clients safekeeping and settlement services. A local custodian primarily focuses on serving a single securities market. If a custodian has access to 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) has further strengthened 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 on behalf of the merchant (i.e. performing for the merchant all the steps necessary for the

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.

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.

As from May 2020, MCE was designated by the Eurosystem as a systemically important payment system (SIPS) according to the criteria included in the ECB SIPS Regulation. The Mastercard Clearing Management System operated by MCE has become the fifth SIPS in the Eurozone, next to TARGET2, EURO1, STEP2 and CORE-FR. For a first time an entity active in the card business area has been designated as a SIPS ; its activities exclusively stem from the card-based transactions under the debit and credit card schemes managed by MCE.

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. PIs 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.

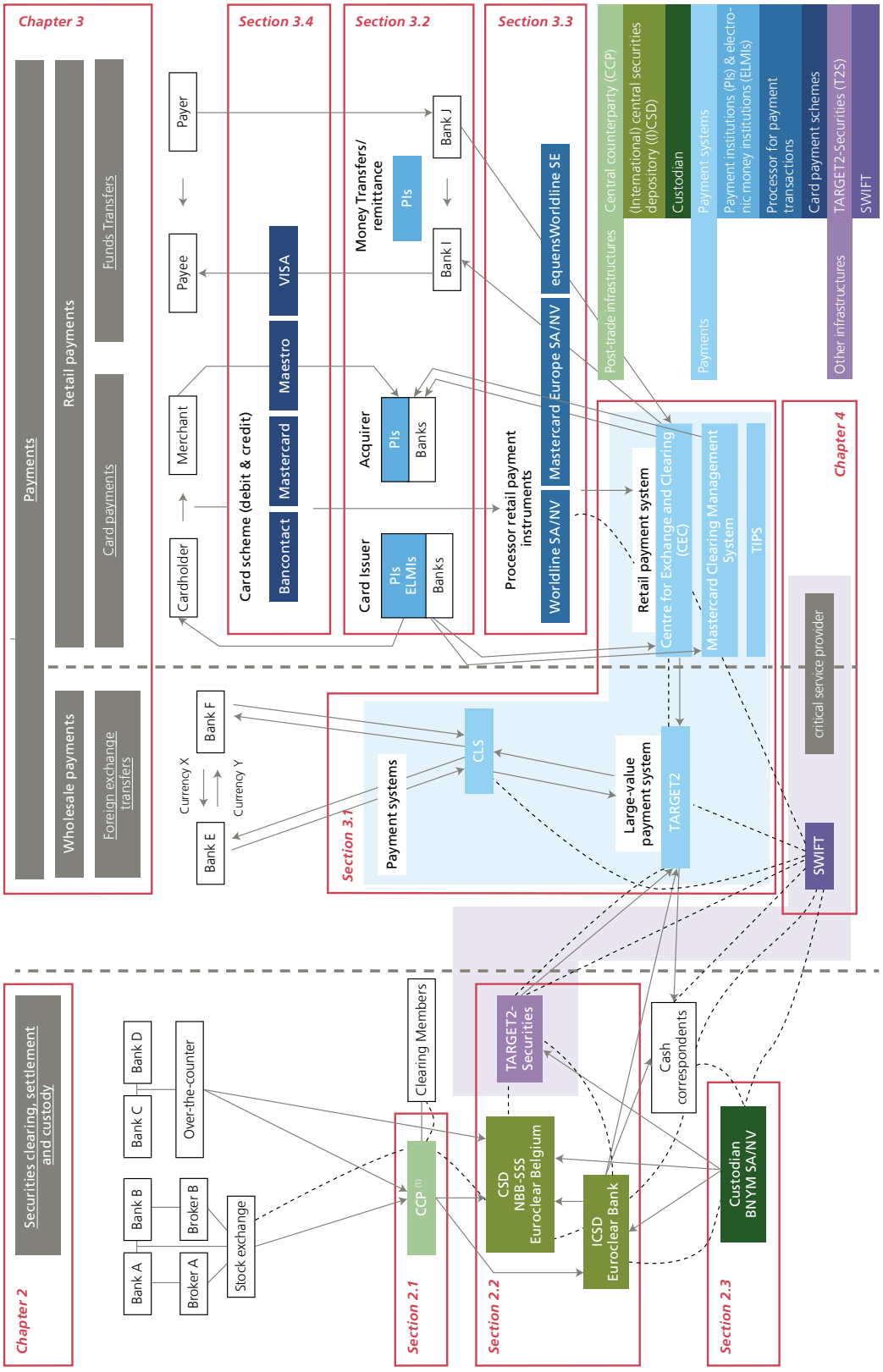
CLS, a settlement system for foreign exchange (FX) transactions is linked to the LVPS systems operated by central banks of 18 currencies (including TARGET2 for EUR), making it possible to settle both legs of the FX transaction at the same time. CLS eliminates FX settlement risk when – due to time zone 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.

Chart 1

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



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

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

Oversight and prudential supervision of FMIs differ in a number of areas[1], 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 Law[2] 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. 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. 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

1 For an overview of those differences, see Table 1 in the Financial Market Infrastructures and Payment Services Report 2020.

2 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.

risks in financial markets. Prudential supervision intends to ensure that institutions are financially robust at micro-prudential level, thus helping to maintain the trust of the institution's counterparties and, in this way, promoting financial stability. 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 instead tends to be 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.

As a consequence of such divergences in scope, oversight and prudential supervision rely on different frameworks. For oversight, the PFMIs 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 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. PFMIs) through Regulations in 2012 and 2014 (EMIR[1], CSDR[2]). The Bank has been assigned as the competent supervisory authority for Belgian (I)CSDs, and, as overseer, is also considered as the relevant authority under CSDR[3].

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.

Table 1 below provides an overview of the systems and institutions supervised and/or overseen by the Bank. In addition to the type of services provided, they have been further grouped according to: (i) the type of regulatory role of the Bank (i.e. prudential supervisor, overseer or both) and (ii) the system/institution's international dimension (the Bank as solo authority, international cooperative arrangement with the Bank as lead or in another role). For the systems and institutions established in Belgium which are systemically relevant in other jurisdictions' financial markets or for the financial industry as a whole, the Bank has established cooperative arrangements with other authorities[4]. 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 European Market Infrastructure Regulation (EMIR): Regulation (EU) No. 648/2012 of 4 July 2012 on OTC derivatives, CCPs and TRs.

2 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.

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

4 In line with CPMI-IOSCO Responsibility E (cooperation between authorities). Through this Report, the Bank intends 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 1

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

(January 2021)

	International cooperation		The Bank acts as the sole authority
	The Bank acts as lead authority	The Bank participates under the direction of another authority	
Prudential supervision		Custodian bank The Bank of New York Mellon SA/NV (BNYM SA/NV)	Payment service providers (PSP) Payment institutions (PI) Electronic money institutions (ELMI)
Prudential supervision and oversight	Central securities depository (CSD) Euroclear Belgium International central securities depository (ICSD) Euroclear Bank SA/NV Supporting institution Euroclear SA/NV	Central counterparties (CCP) LCH Ltd (UK), ICE Clear Europe (UK) LCH SA (FR), Eurex Clearing AG (DE), EuroCCP (NL), Keler CCP (HU), CC&G (IT)	Payment processor and payment institution Worldline SA/NV
Oversight	Critical service provider SWIFT	Other infrastructure TARGET2-Securities (T2S)[1]	CSD NBB-SSS
	Payment system Mastercard Clearing Management System[2]	Payment system TARGET2 (T2)[1] CLS	Card payment schemes Bancontact[1] Mastercard Europe[1] Maestro[1]
			Payment processors Mastercard Europe equensWorldline
			Payment system Centre for Exchange and Clearing (CEC)[1]

Post-trade infrastructure	Securities clearing	Payments	Payment systems
	Securities settlement		Payment institutions and electronic money institutions
	Custody of securities		Payment processors
Other infrastructures	T2S		Card payment schemes
	SWIFT		

Source: NBB.

1 Peer review in Eurosystem/ESCB.

2 The NBB and the ECB act jointly as lead overseers (authorities responsible for oversight).

BOX 1

Impact of COVID-19 pandemic on post-trade and payments activity

Post-trade activity

The following graphs compare the impacts observed for the International Central Securities Depository Euroclear Bank (EB) and the global custodian BNY Mellon SA/NV. This paragraph shows how the two institutions' business was impacted by the COVID-19 crisis, although they have different profiles in terms of asset composition (about 50 % of BNYM SA/NV's assets under custody in terms of value consist of equities, while the latter category only accounts for about 2 % of Euroclear Bank's assets held under custody.)

The following graphs show the change in 2020 compared to 2019, using indices with January 2019 as reference point.

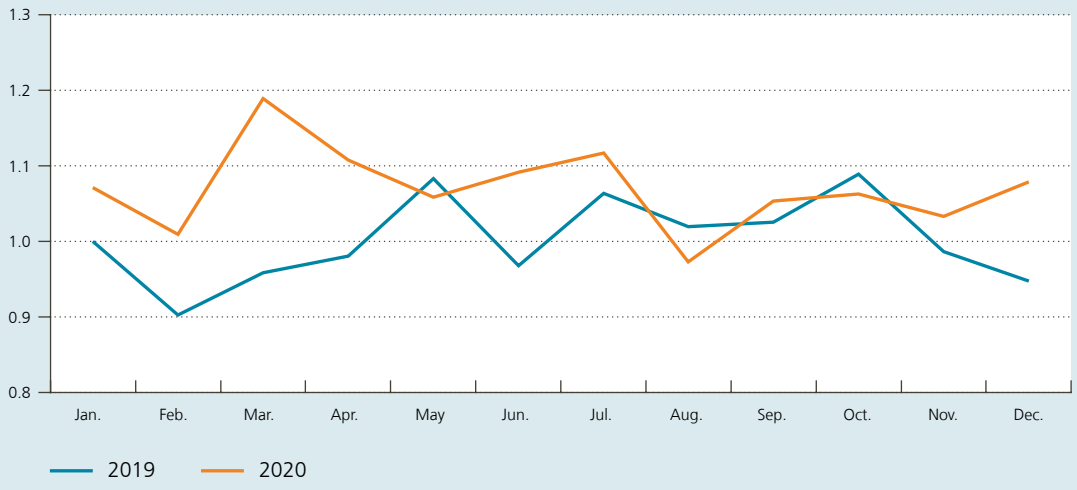
Turnover

The outbreak of the COVID-19 pandemic proved to be a major source of volatility in financial markets. Ashe global rise in COVID cases gained momentum, governments responded with unprecedented measures. The subsequent market turmoil led an increase in both the volume and value of transactions that Euroclear Bank had to settle.

An overall increase in turnover is observed for EB, as shown below. A peak in March, which later smoothed out, is observed for both the number of transactions and the value of turnover.

EB – Value of transactions

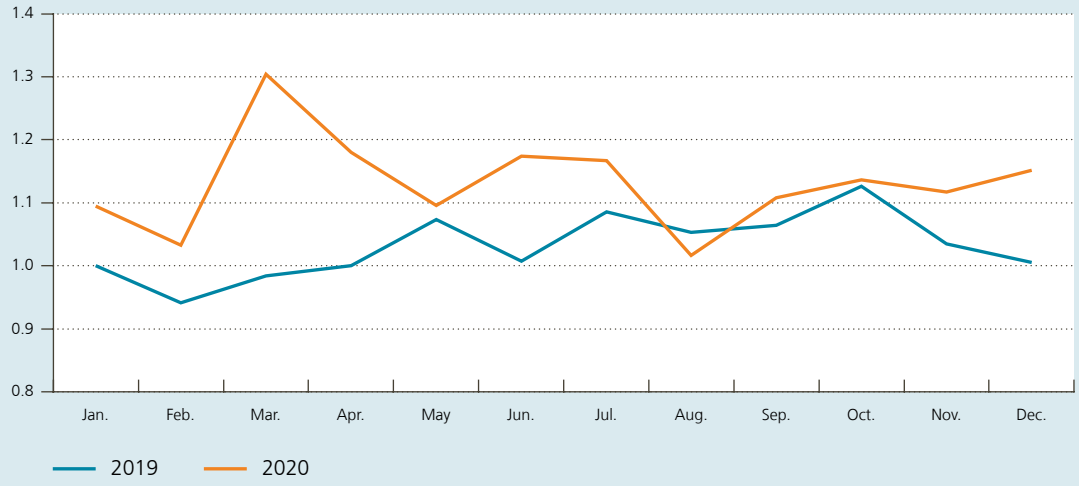
(all data are indexed to January 2019 = 1)



Source: Euroclear.

EB – Number of transactions

(all data are indexed to January 2019 = 1)

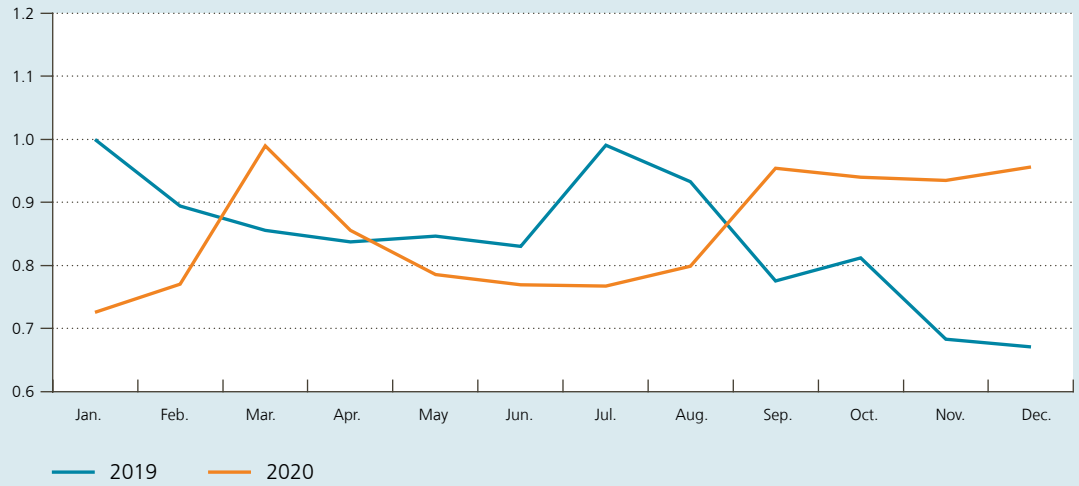


Source: Euroclear.

Similar observations can also be made for BNYM SA/NV as it processes transactions on behalf of its clients. The number and value of transactions jumped significantly in March.

BNYM SA/NV – Value of transactions

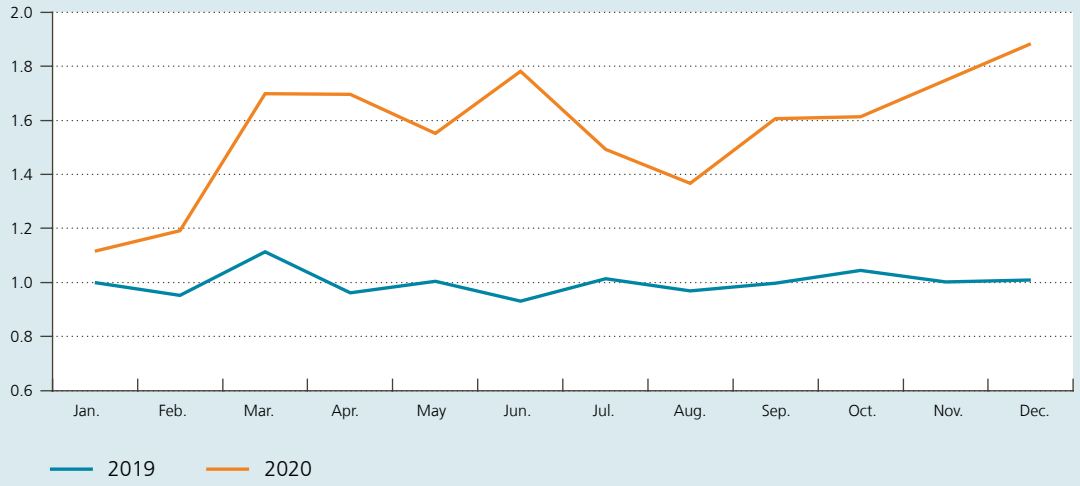
(all data are indexed to January 2019 = 1)



Source: BNYM.

BNYM SA / NV – Number of transactions

(all data are indexed to January 2019 = 1)

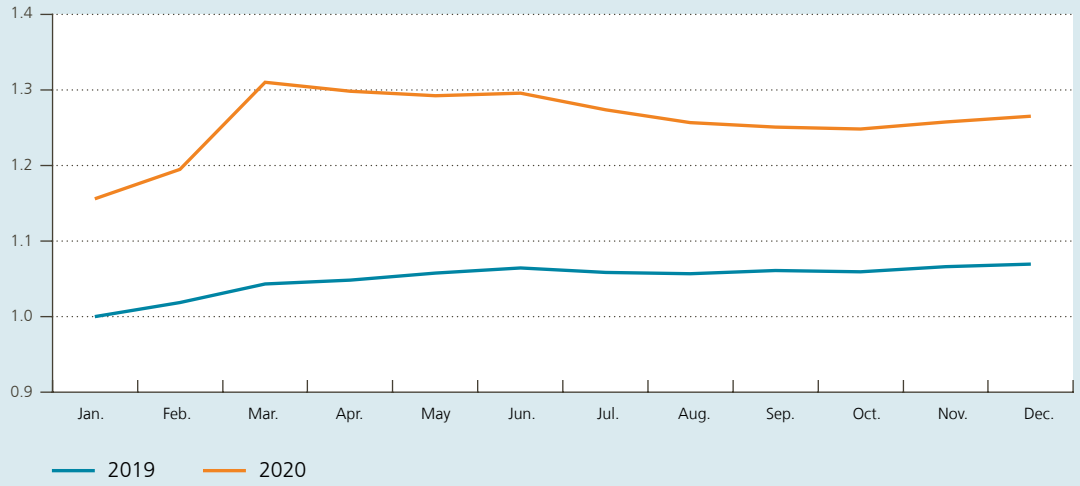


Source: BNYM.

This increase in activity in March 2020 is also reflected in the number of sent messages that were transmitted via SWIFT.

SWIFT – Average daily number of securities related messages sent

(all data are indexed to January 2019 = 1)



Source: SWIFT.

Settlement efficiency

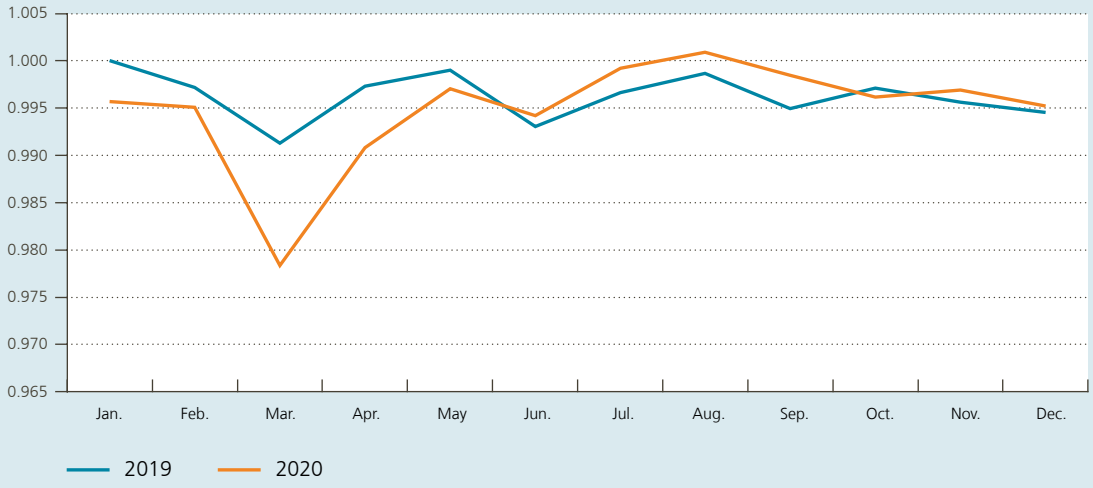
As a result of the larger settlement volumes and participants entering into contingency mode, Euroclear Bank and BNYM SA/NV recorded higher rates of settlements fails. Settlement failure measures the percentage of securities transactions that are not settled on the intended settlement date.

The increase in settlement fails in EB was due to instructions being unmatched or to participants lacking securities. Euroclear Bank exceptionally opened its system on Saturday 28 March 2020 in order to help participants to reduce their backlog.

After the drop in the settlement efficiency (the inverse of the settlement fail rate) in March, the rates for settlement failures returned to normal levels, even reaching higher efficiency in terms of value of transactions compared to the same period the year before. This might indicate that the focus of participants was to settle the higher-value transactions.

EB – Settlement efficiency in value of transactions

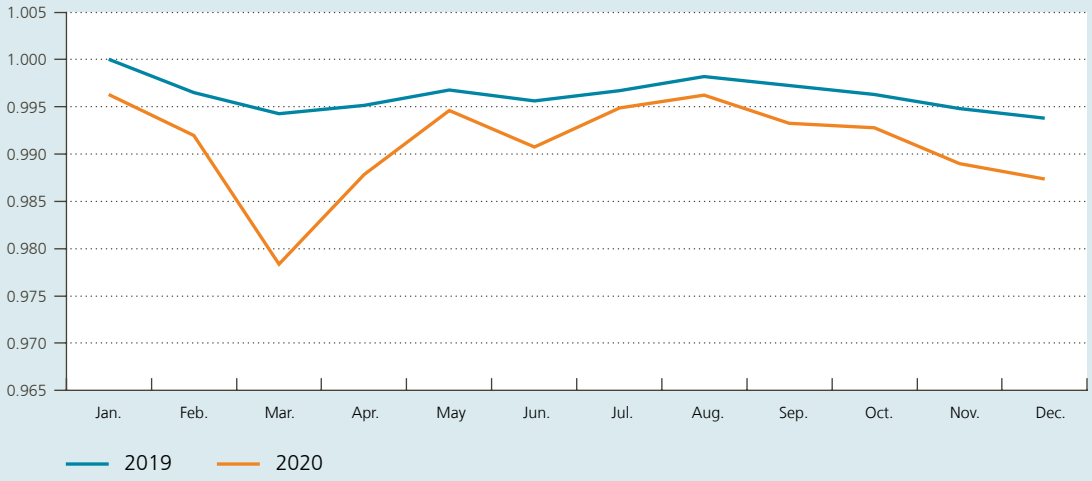
(all data are indexed to January 2019 = 1)



Source: Euroclear.

EB – Settlement efficiency in number of transactions

(all data are indexed to January 2019 = 1)

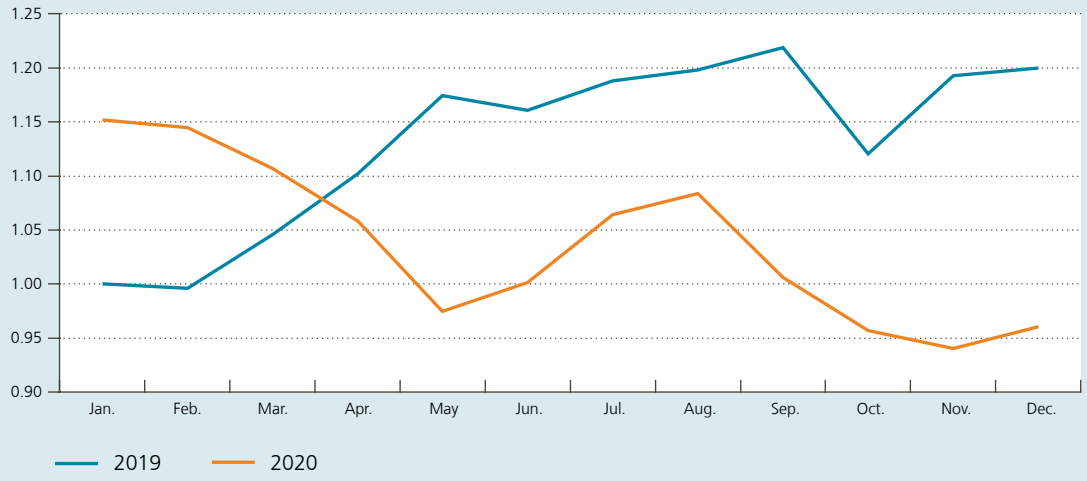


Source: Euroclear.

The market turmoil and the subsequent increase in transactions resulted in an increase in settlement fails at BNYM SA/NV as well. However, the rates for settlement failures did not fully return to normal. Since March, lower levels of settlement efficiency than in the corresponding periods of the previous year have been observed.

BNYM SA/NV – Settlement efficiency in value of transactions

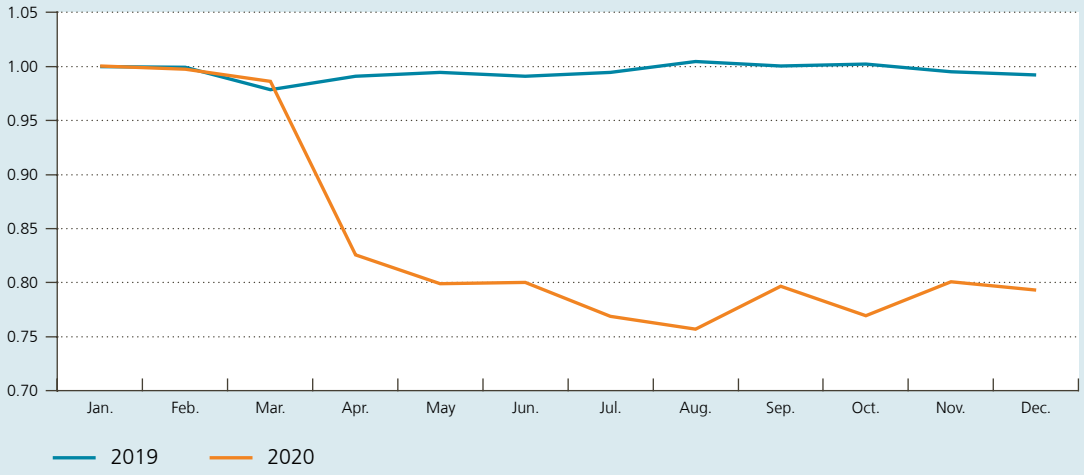
(all data are indexed to January 2019 = 1)



Source: BNYM.

BNYM SA/NV – Settlement efficiency in number of transactions

(all data are indexed to January 2019 = 1)



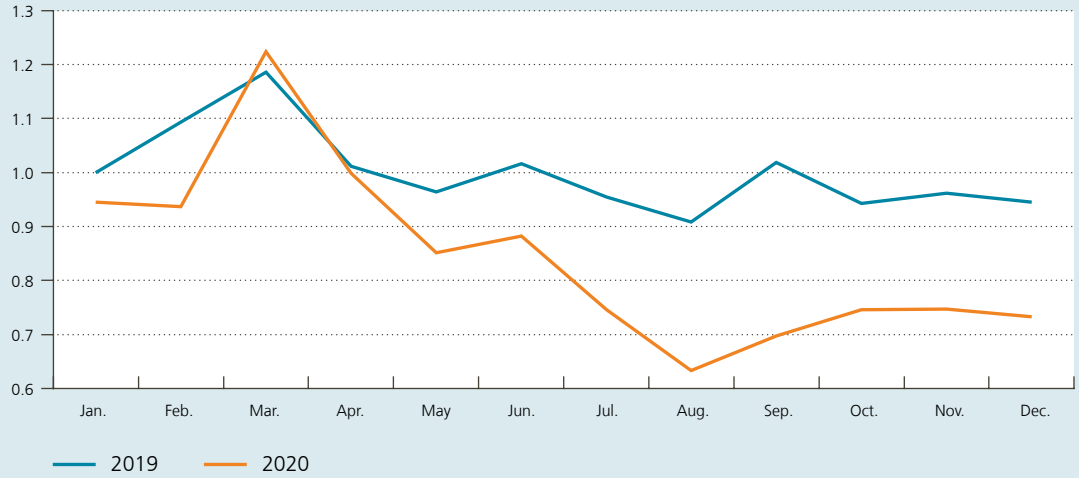
Source: BNYM.

Securities lending

Euroclear provides ancillary services, including securities lending. As this service is fail-driven and aims at optimising settlement efficiency, the amounts of securities lent peaked in March 2020, avoiding a further increase in settlement fails. As the settlement efficiency improved after March 2020, securities lending declined as well.

EB – Securities lending in value of transactions

(all data are indexed to January 2019 = 1)



Source: Euroclear.

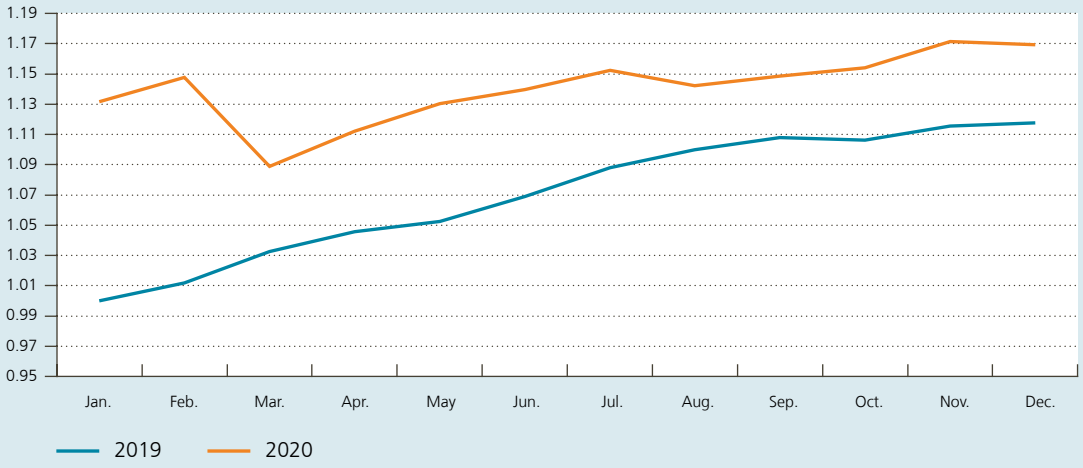
Assets under custody

The March 2020 crash in the prices of securities from companies that were affected by the COVID-19 pandemic and government lockdown measures is reflected in the value of securities held by participants in the books of Euroclear Bank and BNYM SA/NV.

While the value of the assets under custody of Euroclear Bank rose compared to March 2019, there was a considerable drop in March 2020, despite the wider range of different securities held as new issues were brought to the market to raise capital. The market quickly recovered from this surge in the subsequent months.

EB – Assets under custody in value

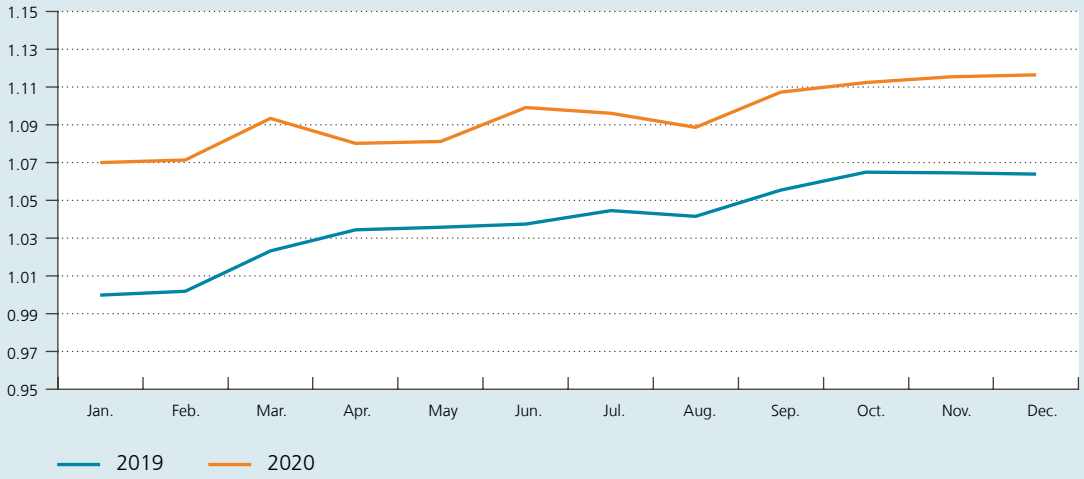
(all data are indexed to January 2019 = 1)



Source: Euroclear.

EB – Assets under custody in number of ISINs

(all data are indexed to January 2019 = 1)

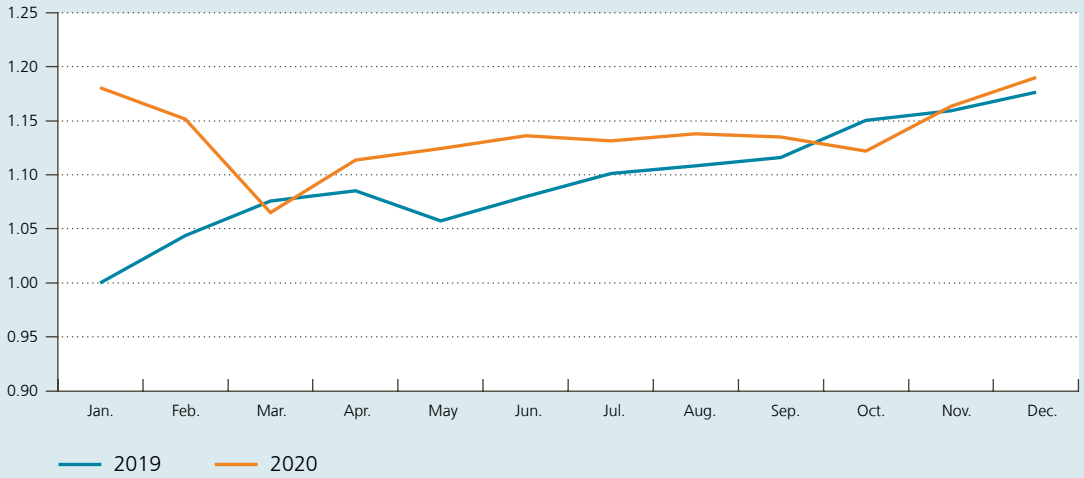


Source: Euroclear.

Similar observations can be made for BNYM SA/NV. The market turmoil as described above resulted in a decline in stock market value of about 35 % (Euro Stoxx 50). This decline impacted the assets under custody at BNYM SA/NV. About 50 % of the Assets under Custody at BNYM SA/NV is equity (as spelled out in the Box in the international dimension about 40 % is EUR and around 30 % is USD). The graph below visualises this impact, in which the quick recovery of the markets is also reflected. By mid-2020, more than half of the loss had been recovered and by the end of the year markets restored at pre-covid levels.

BNYM SA/NV – Assets under custody in value

(all data are indexed to January 2019 = 1)



Source: BNY Mellon.

Payments activity

In 2020, payments were affected by the COVID-19 crisis, too. Not only because of the reduced economic activity but also as a result of changes in consumer preferences, spurning cash for card payments. In Belgium this choice is clearly visible in the 2020 figures for the domestic debit card scheme Bancontact. However, the impact of the economic slowdown is less clear to identify in the volumes processed by the CEC, the Belgian domestic retail payment system.

Bancontact

The COVID-19 crisis influenced card payments in different ways. The reduced economic activity during lockdown periods significantly lowered the need for card payments in physical outlets. More specific pandemic measures targeting activities where payment cards are widely used also negatively impacted the volume of card payments. Among these measures were the closing of bars and restaurants, the restrictions imposed on travel and extensive recourse to teleworking (reducing for example fuel purchases, public transport ticketing, etc.). On the other hand, wider use of e-commerce, aversion to cash and contactless functionalities boosted card payments.

For Bancontact, the domestic and most widely used card payment scheme, these various factors resulted in growth of about 10 % in payments volume (e-commerce, mobile and POS) over 2020 reaching 1.65 billion operations[1]. ATM cash withdrawals amounted to 67 million operations, 34 % down on 2019.

Another notable coronavirus-related trend is the wider use of the contactless functionality. At the end of 2020, contactless payments accounted for 42 % of all payment made with Bancontact cards. This was an increase of 283 % compared to the previous year.

The CEC

With 1496 million operations (including instant payments) processed over the whole year, the CEC's activity shrank by about 5.5 % compared to 2019. However, this drop is the result of multiple factors and the true impact of the COVID-19 crisis cannot be easily isolated.

The clear increase in the use of payment cards shown by Bancontact does not reflect in the CEC figures where the volume of card operations decreases by about 14 % (from 672 million to 580 million) compared to 2019. This evolution is explained by the fact that those operations are not necessarily individual ones but are aggregated and the level of aggregation depends on external factors.

On the contrary, credit transfers (including SEPA Credit transfers and Instant payments) increased by 1.5 % whereas direct debit (SDD Core) decreased in the same proportion.

Two instruments which are used as business payment means, SDD B2B and cheques, were clearly more affected. For instance, the volume of cheques diminished by 40 % which is significantly more than the yearly reduction of about 20 % observed these last years. During the first lockdown, the use of cheques even dropped by 65 %. However, these two payment instruments represent less than 1 % of the CEC volumes and their impact on the global activity of the system is negligible.

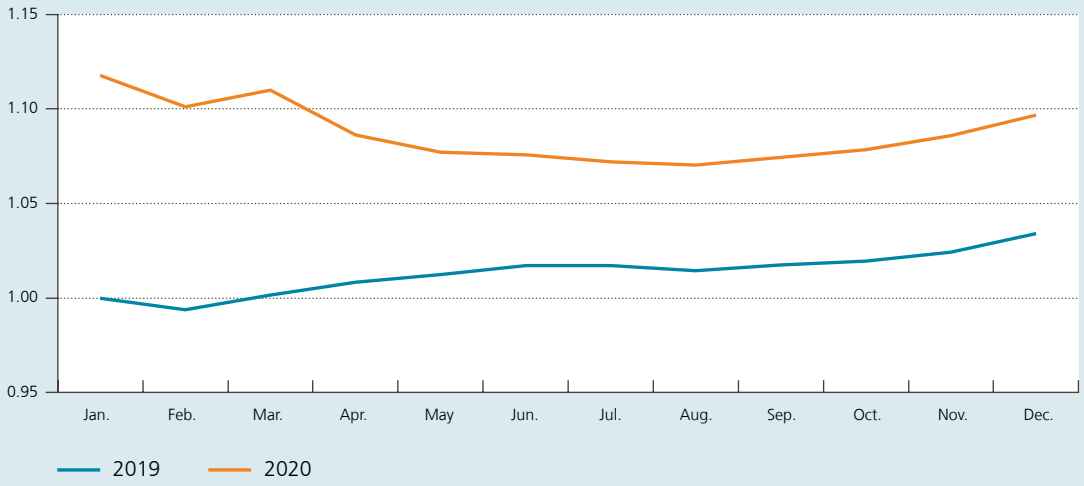
1 Payconiq payments included.

SWIFT

At a global level, the impact of COVID-19 and government measures on payments activity showed a mixed picture as well. The number of payments messages sent via SWIFT clearly slumped since March 2020 (recovering a bit by the end of 2020).

SWIFT – Average daily number of payments related messages sent

(all data are indexed to January 2019 = 1)

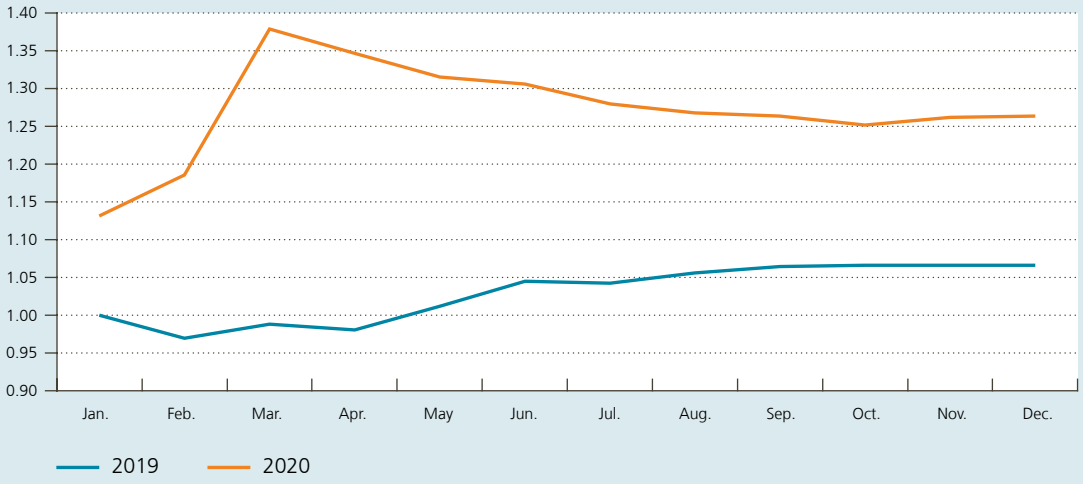


Source: SWIFT.

In contrast, the number of messages related to treasury management increased sharply in March 2020 (while falling a bit back since then).

SWIFT – Average daily number of Treasury related messages sent

(all data are indexed to January 2019 = 1)



Source: SWIFT.

2. Securities clearing, settlement and custody

FMIs and financial institutions that provide securities clearing, settlement and custody services are considered part of the post-trade securities landscape. Systems that clear trades conducted on a stock exchange or concluded between counterparties on the OTC market, as well as the systems that settle the obligations of the buyer and seller of a trade are subject to oversight. In the EU, institutions that operate these systems are subject to EMIR and CSDR supervision. Chart 2 depicts the scope of the Bank's oversight and supervision role in this area.

Section 2.1 covers CCPs. CCPs are subject to both prudential supervision and oversight. While there is no CCP established in Belgium, under EMIR, as of 2021 the Bank will take part in five 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 adequate for covering such risks (i.e. PFMIs). In the EU framework, these principles have been transposed into EU legislation (EMIR and CSDR).

The (I)CSDs established in Belgium have different scopes in terms of activities. While Euroclear Bank provides services in a wide range of securities, securities eligible in Euroclear Belgium are primarily Belgian equities. Under the CSDR, the Bank has been assigned as the sole competent supervisory authority[1] for Euroclear Bank and Euroclear Belgium, and is, as overseer, also considered as 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 of Euroclear Belgium and NBB-SSS are outsourced to TARGET2-Securities (T2S), as in the case of other CSDs in Europe. T2S is not a CSD, but as it provides settlement services to many euro area and some non-euro area CSDs, it is essential that it enables member CSDs to comply with the regulations applicable to them. In line with PFMI Responsibility E (Cooperation with other authorities), the Eurosystem has set up the T2S Cooperative Arrangement to ensure that all authorities with a legitimate interest in the smooth functioning of T2S are involved, including the overseers and market authorities of CSDs that have signed the T2S Framework Agreement, in coordination with the ECB and ESMA. The authorities assess both the general organisation of T2S as a critical infrastructure (i.e. technical platform, legal basis, governance structure and comprehensive risk

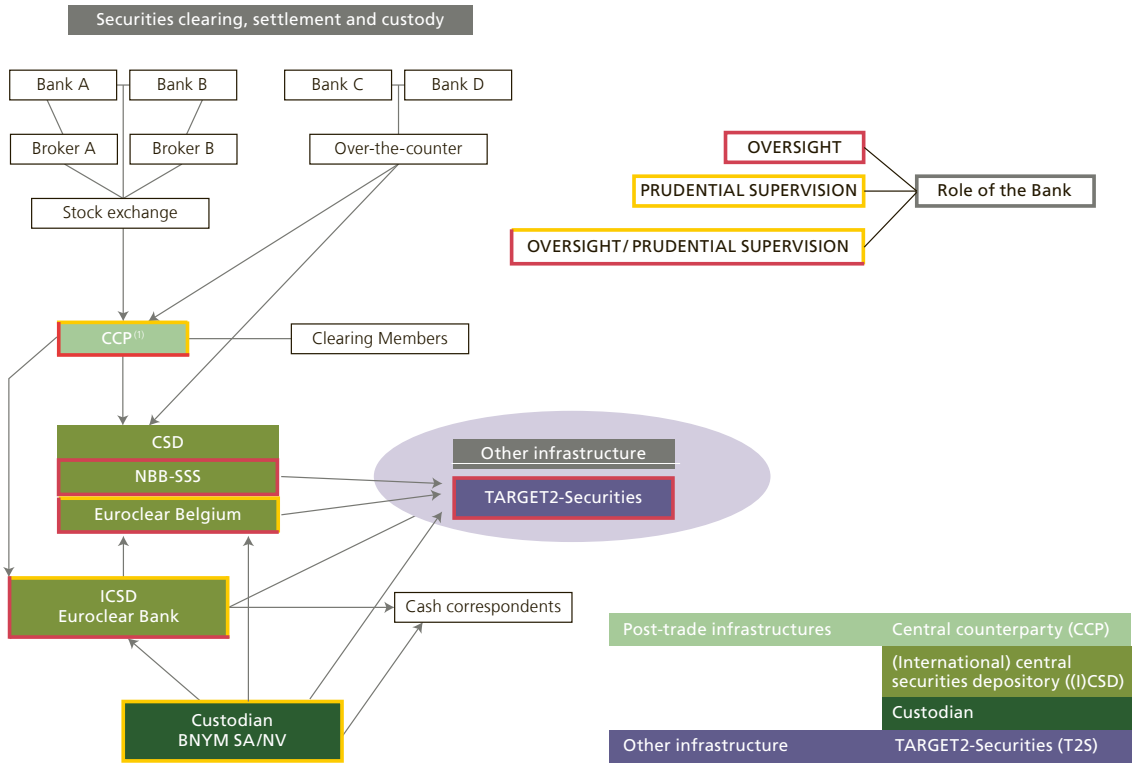
1 For the following aspects, the Bank consults the FSMA, which retains its competence as market authority: rules on conflicts of interest, record-keeping, requirements concerning participation, transparency, procedures for communicating with participants and other market infrastructures, the protection 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.

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

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

Chart 2

Scope of the Bank's oversight and prudential supervision role in the post-trade securities landscape



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

There are no CCPs located in Belgium but some foreign CCPs are used by Belgian financial institutions for clearing, or use Belgian FMIs for settlement (see chart 2), and therefore the Bank closely follows up developments regarding CCPs.

In November 2020, the Financial Stability Board (FSB) further elaborated its CCP resolution guidance with the publication of the Guidance on Financial Resources to Support CCP Resolution and on the Treatment of CCP Equity in Resolution.[1]

1 Available at https://www.fsb.org/2020/11/guidance-on-financial-resources-to-support-ccp-resolution-and-on-the-treatment-of-ccp-equity-in-resolution/.

The FSB, CPMI and IOSCO engaged to conduct further work on CCP financial resources through their respective committees and to consider the need for a policy on the use, composition and amount of financial resources in recovery and resolution to further strengthen the resilience and improve the resolvability of CCPs in default and non-default loss scenarios.

In August 2020, the FSB published a questionnaire on Continuity of Access to FMIs for firms in resolution[1] to streamline information collection and support resolution planning, which should enhance the ability of the administrator of a resolved bank to adequately manage its resolution that typically requires access to FMIs (for instance, to sell securities, transactions need to go through a CCP for clearing and a CSD for settlement – see chart 2 for an overview of the role of FMIs).

The CCP's ability to handle a clearing member's default is essential from a prudential risk perspective. So, its ability to re-establish a balanced book by auctioning the positions of the defaulter to surviving clearing members is key. In June 2020, CPMI and IOSCO published a final paper with considerations on what constitutes a successful auction. The industry is being asked to make further progress on effective auction practices for OTC derivatives positions.

In the EU, EMIR, which sets out the obligations for market participants' clearing derivatives[2] besides the requirements for CCPs and their supervision, has been amended by the EMIR 2.2 Regulation that entered into force on 1 January 2020. EMIR 2.2 improves consistency of supervisory arrangements for CCPs established in the EU and enhances the EU's ability to recognise and supervise systemically important third-country CCPs[3]. While the primary role of the EU CCP's national competent authority is maintained, a wider mandatory consultation of ESMA on regulatory compliance, and an enhanced role for the CCP supervisory college is set. Central banks that issue EU currencies are also being given a bigger input. EMIR 2.2 also includes the possibility to require – via a Delegated Act – the relocation to the EU of so-called "substantially systemically important" activities of third-country CCPs.

The technical legislation for executing EMIR 2.2 is being further elaborated[4]. In December, a delegated act related to the composition, functioning and management of CCP supervisory colleges was published. In October, ESMA issued a market consultation paper making proposals to determine in what cases the national CCP competent authority has to consult the CCP college.

In December, ESMA also issued a time-limited recognition, until mid-2022, of the UK CCPs LCH Ltd, ICE Clear Europe Ltd and LME Clear Ltd[5] preventing these CCPs from losing their authorisation as a Union CCP overnight and allowing EU clearing members to retain access to them during the post-Brexit transition period.

In January 2021, the EU Regulation on CCP recovery and resolution was published[6]. 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. CCPs will have to draw up or adapt their recovery plans as required.

1 Available at https://www.fsb.org/2020/08/fsb-continuity-of-access-to-fmis-for-firms-in-resolution-streamlined-information-collection-to-support-resolution-planning/.

2 Most notably a clearing obligation applies, covering standardised interest rate swap contracts in the most relevant currencies, and index-linked credit default swaps.

3 In September, the Commission adopted delegated acts on when a third-country CCP is considered systemically important and on the comparable compliance regime, allowing a CCP to comply with EMIR requirements by complying with the regulations and requirements of its home country if ESMA assesses them as satisfactory, were published. See https://ec.europa.eu/info/law/derivatives-emir-regulation-eu-no-648-2012/amending-and-supplementary-acts/implementing-and-delegated-acts_en.

4 An overview of EMIR implementing and delegated acts is available at https://ec.europa.eu/info/law/derivatives-emir-regulation-eu-no-648-2012/amending-and-supplementary-acts/implementing-and-delegated-acts_en.

5 Available at https://www.esma.europa.eu/press-news/esma-news/esma-recognise-three-uk-ccps-1-january-2021.

6 Regulation (EU) 2021/23 of the European Parliament and of the Council of 16 December 2020 on a framework for the recovery and resolution of central counterparties and amending Regulations (EU) No. 1095/2010, (EU) No. 648/2012, (EU) No. 600/2014, (EU) No. 806/2014 and (EU) 2015/2365 and Directives 2002/47/EC, 2004/25/EC, 2007/36/EC, 2014/59/EU and (EU) 2017/1132, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2021:022:TOC.

Member States will designate a national CCP resolution authority to resolve a CCP if necessary, which will establish a CCP resolution college to advise on resolution plans and CCP resolvability assessments.

Prudential and oversight approach

In July 2020, ESMA published the results of its third supervisory stress test for EU CCPs[1]. 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 shocks. While the stress test's scenarios were prepared before, they were generally found to be of comparable severity with the stress events at the start of the COVID crisis. The test also included a concentration stress test which showed that, for most asset classes, there is indeed concentration in one or two CCPs, and that the ensuing simulated market impact (i.e. the liquidation cost) for equity and commodity trades was not always sufficiently covered by margin add-ons. Despite this finding, ESMA found the system to be resilient on the whole.

1 Available at https://www.esma.europa.eu/press-news/esma-news/esma%E2%80%99s-third-eu-wide-ccp-stress-test-finds-system-resilient-shocks.

Table 2

EU CCP supervisory colleges with the Bank's participation

CCP[1]	Main clearing services and relevance for Belgium	Direct Belgian clearing members[2]	EMIR criteria for the Bank's participation in the CCP's supervisory college		The Bank participates in the Crisis Management Group
			Supervisor of Belgian clearing members contributing – on a country-by-country basis – most to the CCP default fund	CCP settles in a Belgian (I)CSD[3]	
Eurex Clearing AG (DE)	Listed interest derivatives/repos	4 ■ Belfius Bank; ■ MeDirect Bank; ■ BNP Paribas Fortis; ■ KBC Bank	✗	✓ (EB)	✓
LCH SA (FR)	Euronext cash and derivatives trades (including Euronext Brussels) / repos	8 ■ Axa Bank Belgium ■ Banque Degroof Petercam; ■ Belfius Bank; ■ BNP Paribas Fortis; ■ Delen Private Bank; ■ KBC Bank ■ Leleux Associated Brokers; ■ Van De Put & Co Private Bankers	✗	✓ (EB, EBE, NBB-SSS)	✓
CC&G (IT)	National CCP of Italy	none	✗	✓ (EB)	✗
Euro CCP (NL)	Main European stocks	none	✗	✓ (EB)	✗
Keler CCP (HU)	National CCP of Hungary	1 ■ KBC Securities Hungarian branch	✓	✗	✗

Source: NBB.

1 Under European rules, EU CCP supervisory college participation is reassessed annually on the basis of the criteria set out in Article 18 EMIR. The NBB participates in the colleges based either on its capacity of supervisor of a CSD that the CCP settles in, or as supervisor of clearing members of the CCP that contribute – on a country-by-country basis – most to the default fund.

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

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

Post-Brexit, the Bank continues to be involved in five EU CCP supervisory colleges (see table 2) including in Eurex Clearing AG in Frankfurt that clears euro-denominated repos and LCH SA in Paris that clears the Euronext Brussels markets and euro repos. The Bank is also expected to take part in the third-country CCP supervisory college to be set up under EMIR 2.2, and where information will be shared on these CCPs.

Supervisory priorities in 2021

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

The Regulation on CCP recovery and resolution requires Member States to set up national CCP resolution authorities that will develop plans in case of CCP resolution events and establish resolution colleges. 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. In addition, a continuing priority, common with other FMIs, is CCP operational risk management, and in particular cyber risks.

Finally, new services, 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 rules, the conditions under which a college can escalate a file to ESMA for steering have been eased, and a college majority is now able to include specific guidance in its opinion, besides merely providing a positive or negative vote.

2.2 (I)CSDs

Changes in regulatory framework

According to CSDR Article 75, by 18 September 2019, the European Commission should have reviewed and prepared a general report on CSDR, for submission to the European Parliament and Council, together with any appropriate proposals for revising the regulation. However, due to the lengthy implementation of CSDR (most CSDR requirements started to enter into force only from mid-2017, and settlement discipline will not come into force before 1 February 2022) and the re-authorisation processes which are still ongoing in some countries, it was considered premature to launch a review of CSDR at that time. However, in the course of 2020, and notwithstanding the fact that not all CSDs have obtained their CSDR licence yet, the European Commission has decided to launch a targeted review of CSDR, for which a public consultation took place until February 2021. The European Commission is expected to report to the European Parliament and Council by the end of the first quarter.

Finally, the entry into force of the CSDR settlement discipline regime has been further postponed to 1 February 2022[1]. This postponement is due to the impact of the COVID-19 pandemic on the implementation of regulatory projects and IT deliveries by CSDs and a wide range of market participants and follows a request from the European Commission.

Following the publication of the PFMIs, CPMI and IOSCO agreed to monitor their implementation in members' jurisdictions. An assessment has been performed in late 2019 and early 2020 to examine the consistency of implementation of the PFMIs by FMIs concerning the Business Continuity Planning (BCP) practices (Principle 17 (Operational risk), and more specifically the Key Considerations related to Business Continuity). Globally, it is

1 https://www.esma.europa.eu/press-news/esma-news/esma-proposes-further-postpone-csdr-settlement-discipline.

concluded in the report that the practices are consistent with the expectations regarding business continuity planning laid out in Principle 17 of the PFMI in many aspects. It should be mentioned that FMIs' BCPs include a pandemic scenario. The BCPs are reviewed at least annually and are regularly tested, though some improvements have been identified.

The Digital Operational Resilience Act (DORA, see box 13) and Regulation on Markets in Crypto Assets (MiCA, see thematic article) are also relevant for CSDs.

Prudential and oversight approach

During 2020, the Bank monitored closely the impact of the COVID-19 pandemic on the (I)CSDs' robustness and performance.

Market volatility in March led to significantly higher settlement volumes and fail rates, which returned to normal after this temporary peak as illustrated in box 1.

The interconnection of different market infrastructures is a necessity for the exchange of financial flows. Such interconnectivity creates also potential contagion risks in the event of a problem at one of the nodes of the chain, impacting other FMIs. Hence, cyber resilience continues to be a top priority for the Bank in its oversight activity with Belgian (I)CSDs. In particular, the implementation of the SWIFT Customer Security Programme (CSP) framework continued to be monitored in 2020.

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.

Data integrity is becoming an important topic among the FMIs, because many threats can jeopardise it, be it malware (e.g. a ransomware, which encrypts the data), or an operational incident where some data are modified unintendedly. However, the potential impact on the financial ecosystem could be significant because of the spread of inaccurate data throughout the chains between FMIs and financial institutions. Belgian CSDs are therefore working on "extreme but plausible scenarios" [1] to improve their business resilience, to recover as quickly as possible, should such an incident occur.

As Euroclear Belgium and Euroclear Bank received their initial CSDR authorisation in 2019, the Bank has prepared the first annual review and evaluation (under CSDR Art. 22) in 2020. For Euroclear Belgium, the Bank consulted the FSMA, the Eurosystem as relevant authority under the CSDR and the competent authorities of the Euroclear Group. The Bank finalised Euroclear Belgium's first review and evaluation in February 2021. The assessment was coordinated with the reviews that the French and Dutch competent authorities did on Euroclear France and Euroclear Nederland respectively, as the operations, governance and rulebooks of the three CSDs – together the ESES CSDs – are aligned to a considerable extent.

For Euroclear Bank, the CSDR review and evaluation will be conducted in the course of 2021. The Bank will consult the FSMA, the Eurosystem and the competent authorities of the Euroclear Group. The outcome of the review and evaluation will in addition be shared with the competent authorities of the countries for which Euroclear Bank is important (see box 2).

1 CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures, June 2016.

BOX 2

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, BoE, BoJ and ECB as observer). The Reserve Bank of Australia is in the process of joining this cooperation	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 (and equities as of 2021) 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 and communication arrangement on the oversight and supervision of the ICSDs Euroclear Bank and Clearstream Banking Luxembourg, under Responsibility E of the PFMIs
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 relevant authority as well. The Eurosystem is also relevant authority for Euroclear Bank, which settles in euro as well.

In addition to the FSMA and the relevant authorities, the competent authorities from countries where Euroclear has a CSD will be involved in the annual review and evaluation process of Euroclear Belgium and Euroclear Bank. The outcome report will be shared with the authorities identified based on the conditions listed in CSDR Article 55(4).

As the CSDR has changed the interactions between the authorities of the Euroclear (I)CSDs, the MoU between the Euroclear Group overseers and market supervisors is being reviewed.

BOX 3

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 2020, Euroclear Bank had 1 641 participants located worldwide. Its participant base consists mainly of non-domestic participants, including almost 100 central banks, 27 CCPs and CSDs, as well as credit institutions, broker-dealers and investment banks.

Apart from its notary function for international bonds (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. Euroclear Bank is connected to more than 50 foreign CSDs as investor ICSD in domestic markets.

Euroclear Bank intends to join TARGET2-Securities (T2S) as a participating (I)CSD. Offering central bank money settlement in euro to participants that are allowed to open a central bank account in TARGET2 (T2) lowers risks that are inherent to commercial bank money settlement. In addition to following up on this project, the Bank will continue to encourage Euroclear Bank to open cash accounts with non-euro central banks in order to further eliminate its credit exposure on commercial banks.

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[1] which can be different from the denomination currency[2].

At the end of 2020, the value of securities deposits held on Euroclear Bank's books on behalf of its participants amounted to € 15.3 trillion equivalent (up from € 14.8 trillion in 2019). After EUR (49 %), USD is the main denomination currency (28 %), followed by GBP (11 %). 5 % of securities deposits are in international bonds, for which issuers can choose the currency or country of issue.

Regarding settlement turnover, the number of transactions settled in Euroclear Bank in 2020 came to 128.8 million (up from 116.3 million in 2019). In value terms, this represents € 575.9 trillion (up from € 544.6 trillion in 2019). 61 % of settlement turnover, free of payment and against payment transactions, was denominated in EUR, after USD (17 %) and GBP (10 %). In terms of settlement turnover per security type, compared to securities deposits, international debt accounts for 245 % while the bulk is composed of other types of securities such as domestic debt and, to a lesser extent, equities or exchange-traded funds.

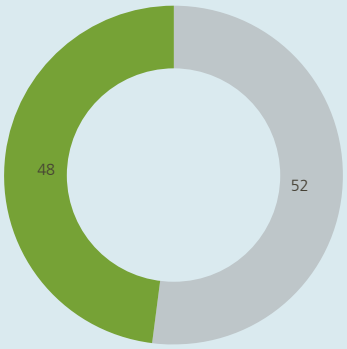
The interconnectivity of Euroclear Bank with other FMIs is a critical component in the Euroclear Group strategy to establish a common pool of collateral assets in which Euroclear Group entities provide

1 A settlement currency is a currency in which cash settlement can take place.
2 A denomination currency is the currency in which the security is denominated. This currency is used as a unit of account for the nominal value of this security, but it is not necessarily used to settle the cash leg of transactions.

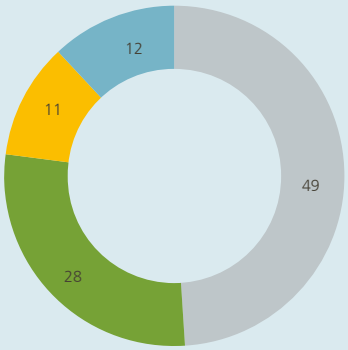
collateral management services as a triparty agent taking over the collateral management tasks (including collateral selection, valuation and substitution) from its participants during the lifecycle of the transaction concluded between two participants. At the end of 2020, at group level, the average daily value of triparty collateral managed by the Euroclear (I)CSDs reached € 1.5 trillion equivalent (up from € 1.3 trillion in 2019).

Composition of securities deposits and turnover in percentage, end of year 2020

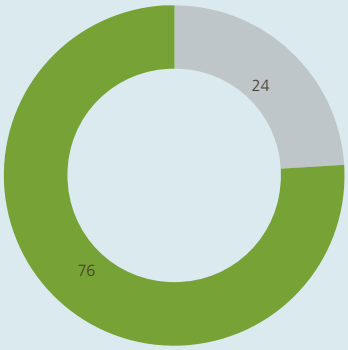
Securities deposits in value-
Breakdown by security type



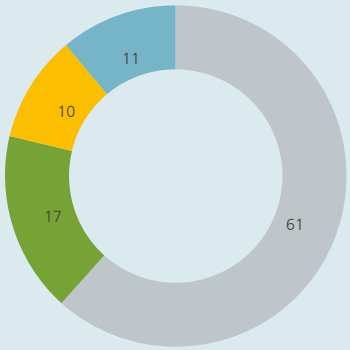
Securities deposits in value-
Breakdown by currency

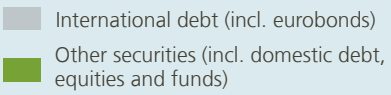


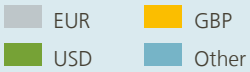
Settlement turnover in value-
Breakdown by security type



Settlement turnover in value-
Breakdown by currency







Source: Euroclear.

Although CSDs operated by members of the ESCB are exempt from the authorisation and supervision requirements of the CSDR[1], certain prudential requirements of the CSDR do, however, apply to them. In the scope of the new regime for granting eligibility to securities settlement systems (SSSs) and links for their use in Eurosystem credit operations, which is based on the compliance of the CSD with the CSDR requirements, the NBB in its role as overseer of the SSS, has conducted a review and evaluation of the NBB-SSS against the CSDR requirements which are relevant from a user perspective and consulted the Eurosystem in this context.

Since June 2020, the NBB-SSS offers DVP settlement in foreign currencies for trades as well as for corporate actions in a fully automated way. In this way, the NBB-SSS supports the settlement of the cash leg in a foreign currency relating to securities denominated in foreign currencies registered in the NBB-SSS. This project implemented an oversight recommendation to avoid settlement risk for securities denominated in foreign currencies.

Given that the daily settlement operations of Euroclear Belgium and NBB-SSS are outsourced to T2S, the Bank is involved in the cooperative oversight of T2S[2].

Because of COVID-19, high market volatility led to progressively higher settlement volumes in T2S, starting from the last week of February 2020 and reaching a historic peak on 16 March 2020 with 1 215 008 transactions settled.

Supervisory priorities in 2021

As required by the CSDR, the Bank as competent authority will perform an annual review and evaluation of the Belgian (I)CSDs that have a CSDR licence. During this review, the Bank will assess whether the (I)CSDs still comply with the requirements laid down in the CSDR. The review will focus on any changes that may have happened with regard to the (I)CSD under review since the last review has been performed. As mentioned above, the Bank will duly consult other authorities and/or inform them of the outcome of the review as required by the CSDR.

Although the NBB-SSS, as a CSD operated by a central bank, is not subject to this CSDR review, the Bank as overseer will perform a targeted review to maintain assurance on NBB-SSS compliance with the provisions of the CSDR that are relevant from a "user perspective"[3].

Since the establishment of Euroclear SA/NV as a financial holding above the (I)CSDs of the Euroclear group[4], the authorities of the Euroclear (I)CSDs set up a cooperation, chaired by the Bank, in line with Responsibility E of the PFMIs to foster efficient and effective communication and consultation in order to support each other in fulfilling the respective mandates with respect to the local Euroclear (I)CSDs. As the current MoU[5] is based on the PFMIs, the authorities of the Euroclear Group (I)CSDs are reviewing it to take into account the new CSDR context.

CSDs' operational resilience will remain a priority in 2021, with cyber resilience as a key focus area. As the pandemic has shown, non-IT aspects are important for operational resilience as well.

The CSDR settlement discipline regime (which was originally due to enter into force in September 2020, and then February 2021) is expected to come into effect on 1 February 2022. The penalty mechanism (developed by T2S) will provide T2S CSDs daily with the penalties to collect and distribute per participant. The preparations for installing the bilateral penalties between participants are ongoing.

1 Under Article 1(4) of the CSDR.

2 The Eurosystem oversees T2S under the lead of the ECB. In line with responsibility E of the PFMI (cooperation with other authorities), the Eurosystem has set up the T2S Cooperative Arrangement to ensure that all authorities with a legitimate interest in the smooth functioning of T2S are involved, including the supervisors and market authorities of the CSDs that have signed the T2S Framework Agreement, in coordination with the ECB and ESMA.

3 The NBB-SSS is eligible for monetary policy operations by the Eurosystem. This means that the Eurosystem accepts securities as collateral in the NBB-SSS. As the Eurosystem is thus a user of the NBB-SSS, it needs assurance that the NBB-SSS is safe to use.

4 See Annex 2 for the organisation chart of the Euroclear group.

5 https://www.nbb.be/doc/cp/eng/aboutcbfa/mou/pdf/mou_2009-10-05_supervisionofeuroclear.pdf.

BOX 4

Brexit: Impact on post-trade intrastructures

As of 1 January 2021, the first Brexit transition period[1] has ended. As the UK is no longer part of the single market, UK institutions could no longer provide services on the continent based on their EU "passport". Similarly, EU institutions would have lost access to the UK if no measures had been taken.

CSDs

In order to continue to provide notary and/or central maintenance services in relation to financial instruments constituted under UK law to either issuers or CSD participants established in the UK, EU (I)CSDs have to obtain UK CSDR recognition. While the recognition is pending, EU (I)CSD that have notified the Bank of England before the end of the first transition period of their intention to continue to provide services in the UK, could continue to provide those services during the subsequent "transitional regime"; i.e. until the UK Treasury makes an equivalence decision for the jurisdiction in which the (I)CSD is established. Following such an equivalence decision, the (I)CSD must submit an application for recognition to the Bank of England within six months in order to continue to provide CSD services in the UK. As securities under UK law have been issued in Euroclear Bank and Euroclear Belgium and these (I)CSDs have UK participants, they have notified the Bank of England (along with other (I)CSDs from the Euroclear group and others).[2] The NBB-SSS, where securities under UK law have been issued, has not notified the Bank of England, as it no longer has UK participants.

As the UK is no longer an EU member state, the Bank of England will no longer be consulted as a relevant authority under the EU CSDR in case it would have been assigned as relevant authority[3] for an (I)CSD. This was the case for Euroclear Bank, where the British pound represents 10 % and was a most relevant currency. The Bank of England was also consulted as competent authority of Euroclear UK and Ireland, being part of the Euroclear Group (as required by CSDR Art 17.6). The National Bank of Belgium and the Bank of England have cooperation arrangements with regard to the oversight on Euroclear Bank and the oversight/supervision of the relationship between the local UK CSD and Euroclear SA/NV, owner and service provider of the Euroclear Group (I)CSDs. Continued cooperation with supervisory authorities of the UK is essential in order to promote the integrity, stability and efficiency of the entities of the Euroclear Group.

There is no CSD in Ireland (which is still an EU member state). Historically, Irish equities have been settled in the UK CSD Euroclear UK & Ireland, while bonds have been settled in the ICSD Euroclear Bank, which is located in Belgium. The EU has temporarily allowed Euroclear UK & Ireland to continue to settle Irish securities, but as a long-term solution, Irish securities have been migrated to an EU (I)CSD, namely Euroclear Bank, in 2021.

1 This transition period is not to be confused with the transition period the EU has granted for UK CCPs and UK CSDs, the transitional regime the UK has foreseen for EU CSDs, or any other transition period.

2 The full list of (I)CSDs that have notified the Bank of England can be found here: https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-market-infrastructure-supervision/list-of-third-country-csds.pdf?la=en&hash=824459A062CBB16DD1C8A42AD2D99A9DC36E3E31.

3 A "relevant authority" as defined in CSR Art. 12 is:
(a) the authority responsible for the oversight of the securities settlement system operated by the CSD in the Member State whose law applies to that securities settlement system;
(b) the central banks in the Union issuing the most relevant currencies in which settlement takes place;
(c) where relevant, the central bank in the Union in whose books the cash leg of a securities settlement system operated by the CSD is settled.

CCPs

UK CCPs have established a dominant position in clearing some financial instruments, such as euro repo transactions based on Belgian bonds. As illustrated in box 3 of the FMI and Payment Services Report 2019, the Belgian euro repo market was predominantly cleared by the UK CCP LCH Ltd. before it started shifting this business to the French CCP LCH SA, which now clears the bulk of this activity. As not all clearing activities have migrated yet (especially for long-term derivative contracts, such shift cannot occur overnight), the EU has temporarily declared equivalence for UK CCPs in order to allow EU clearing members to continue to clear in the UK CCPs to avoid disruption on 1 January 2021. However, the idea is that eventually EU business is cleared in EU CCPs. Legally, UK, American and Asian clearing members could still clear euro repo transactions in a UK CCP, but if the majority of the volumes are cleared in an EU CCP, these institutions may decide to clear in an EU CCP as well, where they will find more counterparties.

Since the UK is no longer part of the EU, there are no longer EMIR supervisory colleges for UK CCPs. Therefore, the Bank will no longer participate in an EMIR college for LCH Ltd. and ICE Clear Europe Ltd. The Bank of England, as competent authority for UK CCPs, may decide to set up "global" colleges for UK CCPs. The Bank is also expected to take part in the third-country CCP supervisory college to be set up under EMIR 2.2 (see paragraph 2.1).

2.3 Custodians

Changes in regulatory framework

There were no changes in the regulatory framework in 2020.

Prudential approach

BNYM SA is considered as a Significant Institution which implies that BNYM SA falls under the direct supervision of the SSM. The majority of the supervisory work is therefore carried out jointly by the Bank and the ECB within the SSM framework. BNYM SA is also subject to specific monitoring by the Bank as regards the specific requirements applicable to custodian banks.

This year, the ECB announced changes to the organisational structure of its supervisory arm to ensure continued effective and efficient supervision of banks in the euro area and beyond. Bank-specific supervision will be structured in three directorates general according to the business models of supervised banks to create more synergies and allow a better comparison of common risks and challenges: Systemic and International Banks (DG/SIB), Universal and Diversified Institutions (DG/UDI) and Specialised Institutions and Less Significant Institutions (DG/SPL). The supervision of BNYM SA will fall under DG/SIB. Next, a dedicated horizontal supervision in the Directorate General Horizontal Line Supervision (DG/HOL) will be created to strengthen risk expertise in the supervision of banks.

As the European subsidiary of BNY Mellon, a US based global systemic bank, BNYM SA is the custodian of the group for European clients and the European gateway to the euro area markets and payment infrastructures.

BNYM SA settles transactions in wide range of currencies, with EUR, GBP, USD an JPY being the main currencies (see box 5 on international dimension). In this framework, a special focus was given to payments activity over the 2020 supervisory year.

BNYM SA has one subsidiary and several branches within Europe through which it operates in the local markets. At the beginning of 2020, BNYM SA had branches in Luxembourg, Frankfurt, Amsterdam, London, Paris, Dublin and Milan. In order to increase the support to Spanish and Iberian clients and to align with the business strategy of European coverage by BNYM SA as custodian for the European clients, BNYM SA has turned the representative office in Madrid into a branch and has established a branch in Denmark in the course of 2020 after receiving regulatory approval of the ECB and the Bank. The Bank reviewed and authorised the incorporation of these two new branches in conjunction with the ECB as a result of its banking licence and autonomously under the custodian bank status.

Besides this, the supervisory work of the Bank as part of the SSM Supervisory Team has focused on the readiness of BNYM SA with regards to Brexit and the compatibility of the business model set-up with a post-Brexit environment. As a global custodian, having a strong international dimension, BNYM operates according to a "follow the sun" model which allows to process clients' transactions and related services around the globe in a continuous way. This is mainly achieved by having established BNYM group entities around the globe, working on common platform and multiple intragroup outsourcing arrangements. The autonomy of functioning of foreign banks established in the Eurozone in the post-Brexit context is an important focus point. Further attention points in this matter are the adaptations to the existing activities, importing of new activities previously offered to EU clients by group entities located outside the EU (such as London), adjustments of booking policies as well as adjustments to the bank's local risk management and governance to deal with the new context resulted from Brexit and related supervisory requirements. The core principles on which the NBB/SSM based its assessment can be found in the Operational Brexit Guidance published on the ECB website [1].

A continuous monitoring of the firm resiliency from an IT and operational perspective is part of the supervisory work. Taking into account the several common characteristics between the business model of BNYM SA and that of FMIs, as well as the central part BNYM SA has as a custodian in the functioning of globalised financial markets, they have to build a high resiliency (amongst others by ensuring sufficient and adequate fall-back capabilities between regional operational centres) in order to meet client expectations, to ensure stability in the functioning of markets and to ensure the global coverage. This became even more important in COVID times.

The COVID crisis brought potential new challenges and attention points for (custody) banks on several domains, such as increased risk levels amongst others resulting from higher on-balance sheet exposure and increased transaction levels in the beginning of the crisis, bank's risk monitoring, operational continuity and resiliency due to lockdowns and material increase in the need for remote working capabilities and the use of regional operational centres to ensure global coverage [2]. A continuous monitoring of the impact of the COVID crisis on the different risks as well as the firm's resiliency was set-up, including regular interaction with BNYM SA as well as the US group entity, and complementary reporting. The yearly regulatory risk assessment ("SREP") included a specific focus on the impact of the COVID crisis on the bank's risk profile as well as on the bank's internal control and risk management capabilities to deal with such unexpected events.

1 https://www.bankingsupervision.europa.eu/banking/relocating/shared/pdf/ssm.supervisoryexpectationsbookingmodels_201808.en.pdf.
2 See also Box 7 of the Financial Market Infrastructure Report 2020 for impact of COVID crisis on custodians.

BOX 5

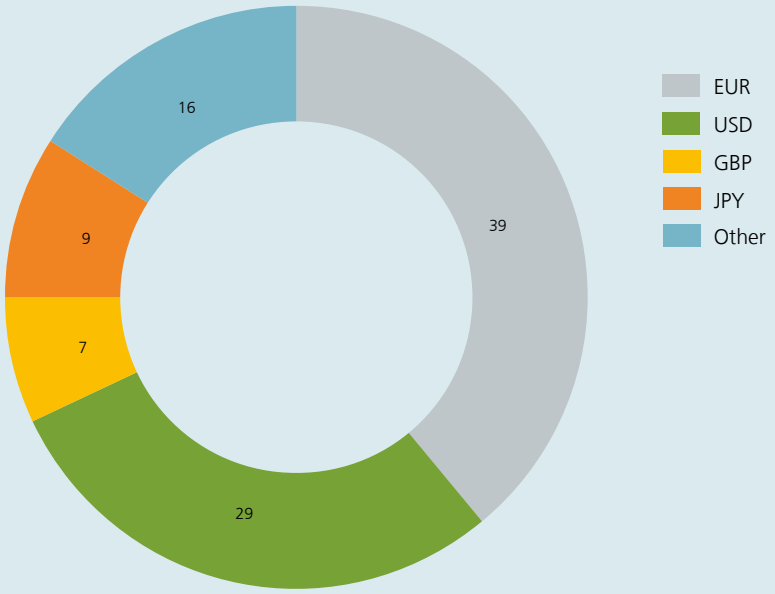
International dimension of The Bank of New York Mellon Group and BNYM SA/NV

The Bank of New York Mellon, a banking group incorporated in the US, is the largest custody bank in the world in terms of assets under custody ($ 41.1 trillion as at December 2020, increased by 11 % compared to last year). It is a global systemically important bank (G-SIB), providing asset and investment management services to institutional customers. The Bank of New York Mellon SA/NV (BNYM SA/NV), the Belgian subsidiary, provides asset services mainly and acts as the groups' custodian for T2S markets and as the global custodian for EU customers. BNYM SA/NV has a non-bank subsidiary in Germany and branches in Luxembourg, the Netherlands, Germany, France, Ireland, Italy, the UK, Denmark and Spain through which it operates in these local markets. BNYM SA/NV qualifies as an 'other systemically important institution' (O-SII) as assessed by the Bank based on the relevant EBA guidelines.

By the end of 2020, BNYM SA/NV served more than 1 100 international, institutional customers on whose behalf it held € 2.9 trillion equivalent assets under custody, denominated in more than 75 different

Assets under custody, per currency

(in %, end of year 2020)



Source: BNY Mellon.

currencies[1]. The increase in the number of customers for the Belgian subsidiary is mainly caused by the migration of customers due to Brexit. The majority of the assets under custody are denominated in EUR (39 %), followed by USD (29 %), JPY (9 %) and GBP (7 %). 51 % of these assets are bonds and 49 % of these assets are shares. In terms of settlement activity[2], BNYM SA/NV processed about 8.4 million transactions worth 32.3 trillion equivalent in 2020; the main currencies are USD (53 %), EUR (22 %), GBP (22 %) and DKK (1 %)[3].

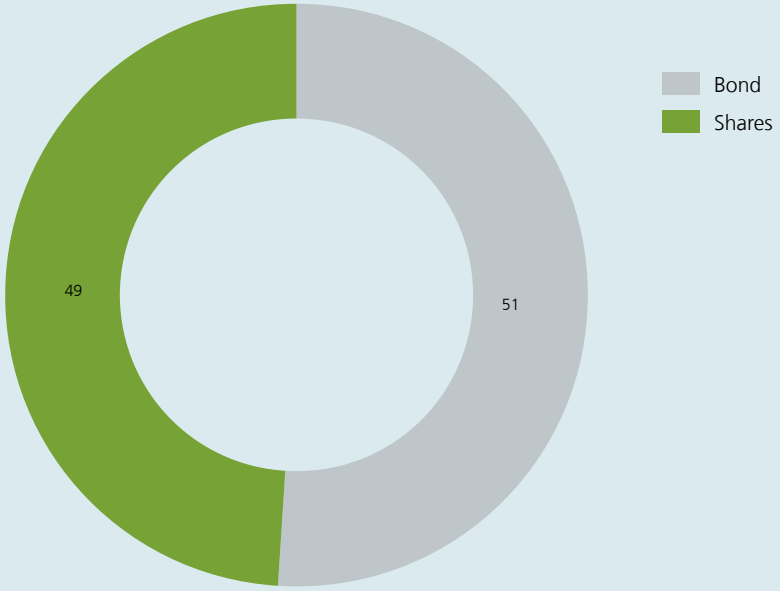
1 Eligible currencies include AED, ARS, AUD, BDT, BGN, BMD, BRL, BWP, CAD, CHF, CLP, CNY, COP, CRC, CZK, DKK, EGP, ETB, EUR, FRF, GBP, GEL, GHS, HKD, HRK, HUF, IDR, ILS, INR, ISK, ITL, JPY, KES, KRW, KWD, KYD, KZT, LKR, MAD, MUR, MXN, MYR, MZN, NGN, NLG, NOK, NZD, OMR, PAB, PEN, PHP, PKR, PLN, PYG, QAR,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

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

3 Compared to last year, the scope of the data related to transactions has changed, this change also impacts the graph Settlement Value by currency.

Assets under custody, per security type

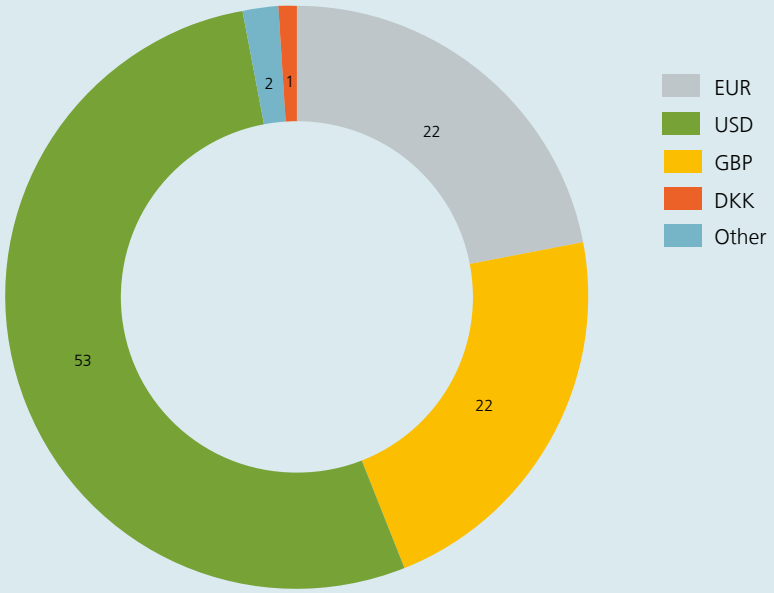
(in %, end of year 2020)



Source: BNY Mellon.

Settlement turnover value, per currency

(in %, 2020)



Source: BNY Mellon.

Supervisory priorities in 2021

The supervisory planning for BNYM SA in 2021 will ensure continuity with the tasks performed last year.

With the approval of a permanent trade agreement between the EU and the UK, the supervisory work on Brexit has completely shifted to the follow-up of the so-called "day-2" solutions (the solutions banks have put in place to do business in Europe after 31 December 2020). In particular, onboarded activities, the legal-entity governance and the legal entity resiliency receive added attention.

As part of their business model, custodians are typically exposed to specific levels of intraday risks. In 2021, supervisors will continue to closely follow-up the modelling and management of intraday credit and liquidity risk.

The regulatory stress testing, held every two years, will take place in 2021 after being postponed following the intensified monitoring of the impact of COVID-19 in 2020. Another consequence of the pandemic is that global interest rates seem to enter a "low-for long" period, which requires a closer follow up of the interest risks on the balance sheet of custodians.

3. Payments

The Bank has broad responsibility in the area of payments and adopts the role of both overseer and prudential supervisor, as illustrated in chart 3 below. These approaches are complementary: while oversight concentrates on the sound and safe functioning of payment systems, payment instruments[1], payment schemes[2] or other payment infrastructures, prudential supervision pursues safe, stable and secure payment service providers delivering payment services to 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. In addition to TARGET2, the Mastercard Clearing Management System operated by MCE (established in Belgium) was designated as a systemically important payment system (SIPS) by an ECB Decision of 4 May 2020 pursuant to Regulation (EU) No. 795/2014 on oversight requirements for systemically important payment systems (ECB/2020/26)[3]. This Regulation lays down the criteria, mainly of a quantitative nature, which, once exceeded, lead to the designation of the concerned entity as a SIPS.

The Bank also participates in the cooperative oversight framework of CLS, a payment-versus-payment (PVP) settlement system for foreign exchange (FX) transactions. The US 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 PSP's (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.

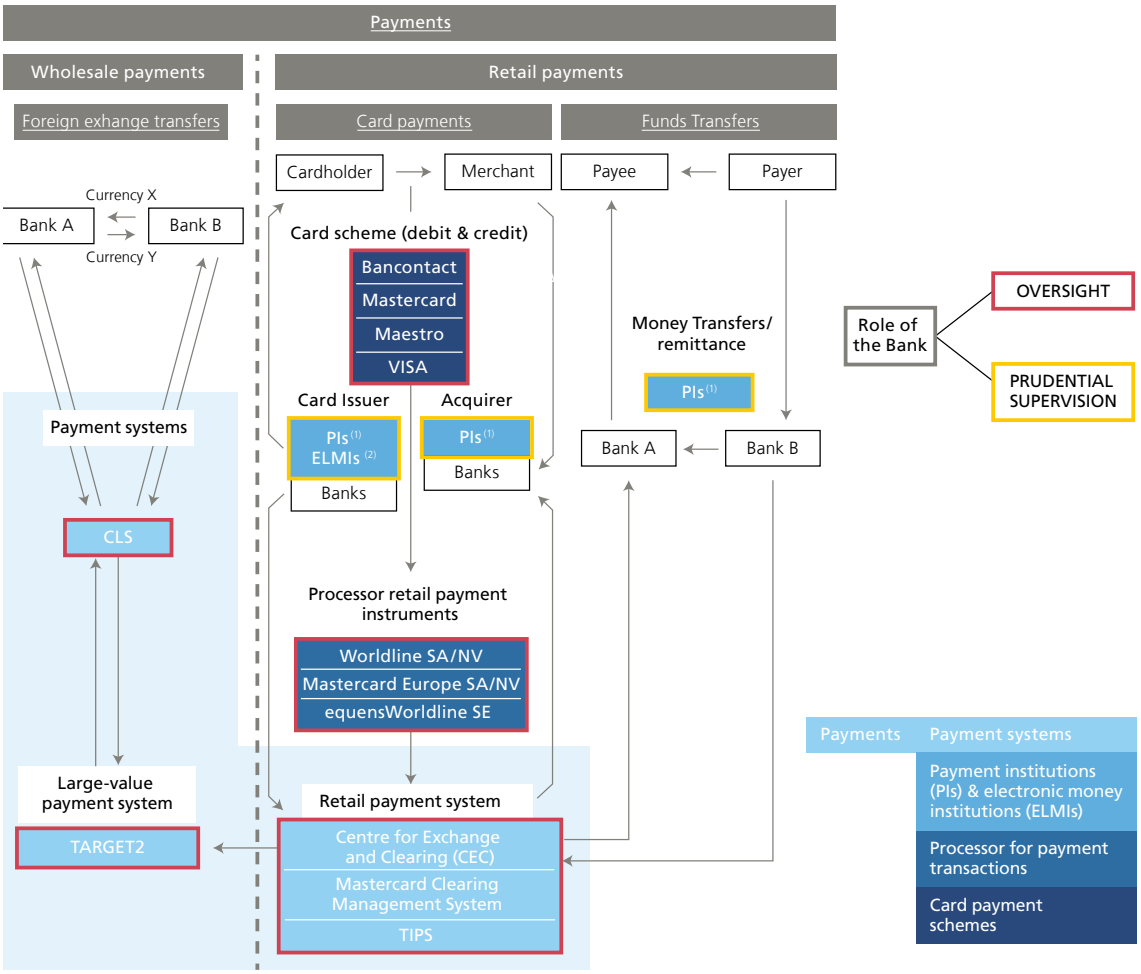
As acquirer[4] and processor of retail payment instruments in Belgium, Worldline SA/NV is subject to both prudential supervision and oversight. The Bank's activities in that respect are covered in section 3.3.

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 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020XB0026.
4 Acquiring card payments is a service whereby a payment service provider contracts with a payee (merchant) to accept and process payment transactions guarantying the transfer of funds to the payee (merchant). The processing part is often performed by another entity.

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).

Chart 3

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



1 Payment institutions (PIs).
2 Electronic money institutions (ELMIs).

BOX 6

The European Commission, the European Central Bank and the NBB unfold their retail payments strategies

The Bank and international regulators have gone through an update of their key priorities in the retail payments area.

In connection with its digital finance strategy, the EC[1] developed a specific retail payments strategy for Europe focusing on four key pillars, which are closely interlinked: 1) increasingly digital and instant payment solutions with pan-European reach; 2) innovative and competitive retail payments markets; 3) efficient and interoperable retail payment systems and other support infrastructures; and 4) efficient international payments, including remittances.

The key objectives laid out in the EC's retail payments consultation were aligned with the Eurosystem's retail payments strategy adopted by the **ECB**'s Governing Council with its main goal to support and foster development of pan-European Point Of Interaction (physical Point Of Sale – POS – + e-commerce) payment solutions. Other major goals consist of a full deployment of instant payments, support for innovation and an innovative payments ecosystem, an improvement of cross-border payments as well as work on eID/eSignature.

At the national, Belgian, level, **the Bank** plays an important role in fostering the modernisation of payment services in order to meet the public policy objectives of safety, efficiency, availability and meeting end-user needs and expectations. The Bank conducted a thorough strategic exercise and concluded on its policy stance on various topics which are aligned with the international regulators' views.

The main action point of the Bank's strategic exercise was to establish a new committee to bring together all the parties involved at the highest level with the aim of ensuring that its policy objectives are ensured under the best possible conditions in Belgium. This **National Retail Payments Committee (NRPC)** is chaired by NBB Director Tim Hermans and members include all relevant stakeholders in the area of the retail payment ecosystem:

- public sector representatives (public institutions in the domains of Finance, Consumer Protection, Economy, Administrative Simplification, Treasury);
- corporate and retail sector representatives;
- consumer representatives;
- representatives of the financial sector entities active in retail payment services (credit institutions, payment and electronic money institutions);
- Belgian financial market infrastructures (FMIs), payment schemes and systemic operators in the field of payments;
- transport sector for cash (CIT, Cash-In-Transit);
- other supervisors/regulating bodies.

1 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a Retail Payments Strategy for the EU (COM/2020/592 Brussels, 24.9.2020).

The Bank is well placed to initiate this, since its powers cover all means of payment, the payment systems/schemes and payment services. The core objective of the NRPC is to facilitate discussion and consultation relating to retail payments in Belgium in order to enable the smooth functioning of the Belgian economy, taking account of public interest considerations. Inefficiencies in the retail payments market may actually have significant negative effects throughout the economy.

By discussing and consulting within the NRPC community, all relevant stakeholders are expected to apply the collective knowledge, experience, and ability to gain a more complete understanding of the retail payment ecosystem. Using this knowledge, members can individually and unilaterally make appropriate decisions regarding their own business risks and opportunities.

The NRPC potentially handles the following non-exhaustive list of topics:

- safe and efficient payment services/activities/instruments and access for domestic and cross-border purposes;
- availability and accessibility of cash;
- acceptance of cash;
- security, transparency and awareness regarding the usage of payment instruments;
- discussion and monitoring of technological developments;
- update on regulatory developments;
- monitoring trends in retail payment activities.

It is the Committee's policy to govern its activities in compliance with the applicable competition laws at all times.

3.1 Payment systems

Changes in regulatory framework

The Belgian and the Eurosystem regulatory frameworks applicable to payment systems were not changed at all in 2020.

Oversight approach

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.

As from May 2020, the Mastercard Clearing Management System (MCMS) operated by MCE (established in Belgium) has been designated as a fourth SIPS with a pan-European reach (while the fifth SIPS has full national anchorage). The activities of MCE as a SIPS stem exclusively from the card-based transactions under the debit and credit card schemes managed by MCE. The combination of this pan-European reach with this strong link to the MCE's scheme activities for which the NBB was the lead overseer since 2008, have led the Eurosystem to appoint both the ECB and the NBB as joint competent authorities for the oversight of this system. The designation of

MCMS as a SIPS stems from MCE fulfilling a number of criteria, listed in the SIPS Regulation itself and mainly of a quantitative nature, referring to market shares, cross-border activities.

The Bank is responsible for the oversight of the CEC, the Belgian domestic retail payment system. The last major change in the system was the launch, on 4 March 2019, of a platform for the processing of instant payments (IP) which was integrated into the existing automated clearing house as an additional functionality. In 2020, the Bank continued to monitor the functioning of the CEC and particularly the IP functionality. No significant incident was observed. Almost 100 million IP operations were processed in 2020 (which represents about 15 % of all credit transfers processed by the system) with daily peaks at more than 500 000 operations.

Supervisory priorities in 2021

Regarding the Mastercard Clearing Management System, the 12-month period following its 4 May 2020 designation as a SIPS, were to be considered as a grace period. Along the latter the NBB and the ECB, with the support of a "joint oversight team" (made up of representatives of the Eurosystem NCBs), have provided support to MCE efforts with a view to render its SIPS compliant with the SIPS Regulation at the May 2021 horizon. The effective official assessment by the Eurosystem of the MCMS compliance has started in May 2021 and is expected to last about one year. As from the same May 2021 milestone, an extended reporting will be expected from MCE as the operator of the MCMS, in terms of activities, incidents and major changes. This SIPS qualification will also entail a set of more formal exchanges between the Eurosystem and representatives of different governance levels and key operational functions (risk management, IT, internal audit, operations & business continuity, change management, etc.) of MCE.

In 2021, the Bank will continue to pay specific attention to the development of the CEC's cyber resilience as well as, for the IP functionality, to the implementation modifications resulting from the ECB Decision on measures to increase the pan-European reach of instant payments.

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 2018[2], 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.

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.

In 2019, the last Royal Decree[1] 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 RTSs[2] (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 2019[3], which is also applicable to 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.

In an amendment to its 2018 guidelines, the EBA updated the guidelines on fraud reporting under PSD2 on 22 January 2020. The Circular of 24 March 2020[4] reflects these changes, which are mainly technical in nature. In addition, further EBA guidelines on ICT and security risk management were transposed by way of the Circular of 16 June 2020[5], which requires all payment and electronic money institutions to report on any operational and security risks as well as applicable mitigating measures. In order to capture the significant changes over the years, the framework Circular was replaced by the Circular of 8 July 2020[6] concerning the prudential statute of payment institutions and electronic money institutions. This Circular gives an overarching overview of the legal framework that applies to payment and electronic money institutions.

1 Royal Decree of 21 March 2019 approving the rules of the National Bank of Belgium on own fund requirements of electronic money institutions.
2 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.
3 Circular 2019_19 on the guidelines of the European Banking Authority of 25 February 2019 on outsourcing.
4 Circular 2020_007 on the guidelines of the European Banking Authority of 22 January 2020 on fraud reporting under PSD2.
5 Circular 2020_24 on the guidelines of the European Banking Authority of 29 November 2019 on ICT and security risk management.
6 Circular 2020_27 on the prudential statute of payment institutions and electronic money institutions.

BOX 7

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. It forms 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

As mentioned in the 2020 FMI and Payment Services Report, 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. This 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 based on non-SCA compliant use of the card details (as printed on the payment card). The second concern related to the technical capabilities in the industry to make 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. Examples 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. 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. The communication protocol best suited to establish this communication is often referred to as EMV 3DS.

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

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).

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".

As the reader may recall, the Bank leveraged on 28 August 2019 this supervisory flexibility option provided by the EBA which resulted in the first half of 2020 in the approval of a roadmap for this migration agreed between the involved stakeholders and published on the Bank's website in early May 2020[1].

Apart from mitigating the two concerns stated above, a key strategy of this migration plan is to migrate incrementally towards full SCA compliance for all card transactions through the use of a mechanism of soft declines whereby a card transaction that is not strongly authenticated is returned to the merchant for authentication providing the merchant with an opportunity to strongly authenticate the cardholder instead of being confronted immediately with a declined card transaction. By incrementally increasing the threshold underneath which this soft decline is applied, the migration plan ensures a gradual uptake of SCA requirements providing the card payment industry, and importantly, e-commerce merchants with ample time to adjust as well as identify and solve any problems that may arise on a technical level.

Following publication of the migration plan in early May 2020, the Bank has actively been monitoring the ongoing march towards a successful implementation of SCA for the online card environment. During the course of 2020, the first concern stated above has been fully mitigated by payment service providers under supervision of the Bank. In relation to the second concern, Belgian payment service providers (issuers and acquirers) have achieved a high level of implementation of the required communication protocol EMV 3DS. It should nevertheless be noted that payment service providers are heavily dependent to a large degree on e-merchant websites (both domestic and – even more so – foreign) making the necessary technical implementations in order to render SCA-compliant card transactions possible on their websites and in their mobile applications.

In supervising the phased roll-out of SCA for these card transactions, the Bank pays special attention to the situation in neighbouring countries with which Belgian cardholders interact frequently in the field of e-commerce. Taking into account the impact of the COVID-19 pandemic on the importance of e-commerce for Belgian cardholders and of not disrupting e-commerce, the Bank therefore seeks to avoid unnecessary friction in the online e-commerce market for Belgian cardholders. Accordingly, the Bank has sought and continues to seek to ensure a high level of alignment, wherever and whenever feasible, with neighbouring markets in supervising and enforcing SCA for the e-commerce card industry. The current state of the SCA migration plan reflects this endeavour.

It should furthermore 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.

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

(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.

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. Provided this dedicated interface meets certain requirements, it can be exempted from the requirement to foresee a contingency mechanism.

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 is rather incrementally continuing as new versions of the dedicated interface are brought into production.

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 clarifies a number of obstacles identified in the market, including requiring multiple SCAs, the manual entry of the International Bank Account Number (IBAN) in the ASPSPs' domain, or imposing additional checks on the consent given by the customer to the TPP. The Bank confirmed that it shares the stated view of the EBA and integrated 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 expected the sector to have complied with this Opinion by 31 December 2020 at the latest. This deadline was shared by the majority of national competent authorities (NCAs) in the European Economic Area (EEA).

Throughout 2020, as in 2019, the Bank engaged proactively with Belgian ASPSPs in order to clarify the relevant legal framework and its interpretation.

To assess the individual readiness of each ASPSP with the end-of-2020 deadline, the Bank sent out questionnaires to all concerned ASPSPs in the third quarter of that year. From the responses and subsequent bilateral meetings held with ASPSPs, it could be concluded that several obstacles in dedicated interfaces were prevalent at that time. These include, among other things, lack of support for all payment functionalities (e.g. instant payments, bulk/file payment and international payments), lack of incorporation of certain authentication procedures (e.g. face/fingerprint recognition, Itsme), lack of implementation of an app-to-app and web-to-app redirection with as a consequence that certain payments cannot be executed and/or certain functionalities are off-limits to TPPs dependent on the

channel in which the TPP is active (mobile or web), the failure to implement a contingency mechanism if the dedicated interface is not exempted from it and the existence of other obstacles as listed in the aforementioned Opinion, e.g. requiring multiple SCAs in the redirection flow, rendering account selection difficult, verifying payment service user consent at ASPSP level and requesting additional TPP registrations.

The Bank emphasised to ASPSPs that the deadline had to be met and obstacles should have been removed by 31 December 2020. The Bank continues to prioritise the verification and monitoring of the removal of all obstacles as listed above from dedicated interfaces in order to ensure that continued non-compliance does not prevent TPPs in Belgium from offering RTS-compliant payment initiation and account information services and to ensure a level playing field among and equal treatment between compliant and non-compliant ASPSPs. In cases of continued non-compliance, the Bank may have to consider what steps would be most appropriate to mitigate the situation.

Supervisory Priorities in 2020 and 2021

The Bank's main supervisory activities in 2020 consisted primarily of i) authorisation of new payment institutions, electronic money institutions and registration of limited networks, ii) monitoring implementation of the requirements related to the RTS on strong customer authentication and common and secure communication within the Belgian market[1] and iii) completing the final changes to the prudential supervision model as set out in PSD2.

The number of payment institutions/electronic money institutions under supervision has risen over the past year from 31 to 37[2], led by a notable increase in firms, both start-ups and incumbents, wishing to apply for the required authorisation to be able to provide payment initiation and account information services. Institutions offering money remittance services have also expressed significant interest. This could be explained as a result of Brexit and the expiry of the transition measures, leading many enterprises to finalise their move to the European Union in order to continue providing their respective services. The number of electronic payment institutions remained stable with seven institutions under supervision in 2020.

Within this context, the Bank observes the following trends with regards to the business models of new service providers:

- collaboration between traditional banks and financial institutions with up-and-coming FinTech players;
- consolidation of specialised payment providers in the card payments sector;
- continued interest in the provision and issuance of crypto-currency and assorted services.

Regarding the first trend, the Bank has observed that a growing number of banks have partnered or acquired FinTech enterprises providing account information and payment initiation services. Even as the possibilities of open banking are unfolding, the landscape is highly fragmented and has ample opportunities for consolidation, a trend which is seen in Belgium and the rest of the European Union.

1 See Box 7.
2 33 Reasons, Jubilee Services, Sendwave, GuiSquare, Together Connected, PagoFX.

The second observed trend relates to the increase in consolidations across Belgian card payment providers, more specifically expense cards. Following the entry into force of the Interchange Fee Regulation (IFR), caps have been imposed on consumer debit and credit cards, leading to lower profitability for providers. In order to deal with mounting costs, mainly in terms of processing, mergers in the sector seek to restore profitability.

Recent activity in crypto-markets as well as regulatory developments within the EU have fuelled a barrage of questions regarding crypto-currencies. In the absence of common European legislation, whereby some countries[1] have implemented national solutions, uncertainty remains rife. So, the provision or use of crypto-services is exposed to significant risks for enterprises and consumers alike. As a matter of policy, the Bank takes a prudent stance towards the offering of crypto-assets in Belgium while awaiting the MiCA framework (see thematic article) to which it contributes to via the appropriate regulators' fora.

In the coming year, several of the recently implemented changes will be expanded upon. The installation of a team of inspectors has allowed the Bank to organise an in-depth review of asset segregation among regulated payment institutions and institutions for electronic money. New reporting requirements will also support a scale-up of regulatory supervision, including in new areas such as (critical) outsourcing, which will be reported on for the first time by all regulated entities.

Concerning the monitoring of 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 full deployment of payment initiation and account information services within the market.

For SCA, the focus will be on ensuring that the migration plan continues to be 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 adherence by ASPSPs to the 31 December 2020 deadline and the effective removal of remaining obstacles in 2021 in order to ensure the creation of stable and fully functional dedicated interfaces enabling the provision of TPP services in the Belgian market.

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.

1 Such as Germany and France.

BOX 8

Money remittance in Belgium

Money remittance is a long-established payment service regulated in Europe by the second Payment Services Directive (PSD2), where funds are received from a payer, without any payment accounts being created in the name of the payer or the payee, for the sole purpose of transferring a corresponding amount to a payee or to another payment service provider acting on behalf of the payee, and/or where such funds are received on behalf of and made available to the payee. Remittances are playing an increasingly large role in the economies of small and developing countries.

In 2019, two money remittance companies were granted a licence by the Bank, and two more in 2020 At the end of 2020, nine money remittance companies were listed as a Belgian payment institution. The Belgian payment institutions have an agent network of 253 agents in Belgium and 8 312 agents[1] in other EEA countries, an increase of 4 %. In addition to the 253 Belgian agents, 1 586 agents of other European payment institutions are active in Belgium.

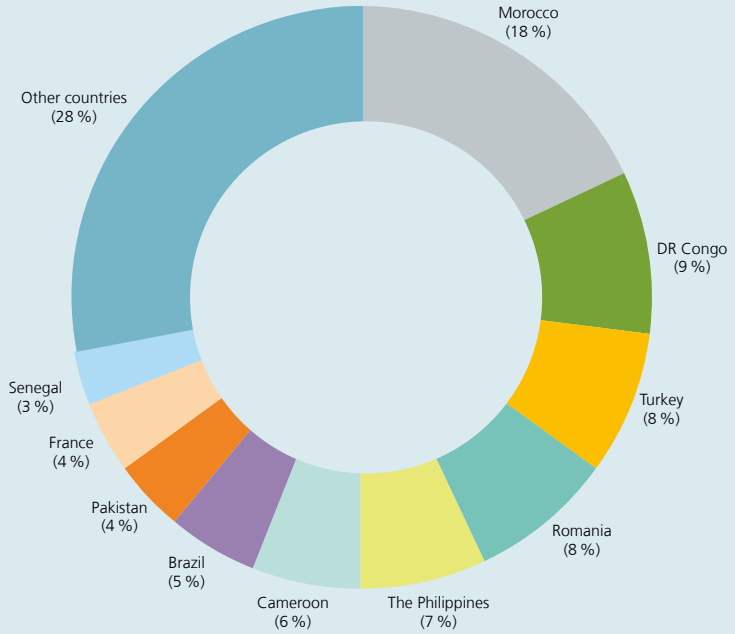
1 91.3 % of the agents work on behalf of Moneygram International, which re-located from the UK to Belgium at the end of 2017, because of Brexit.

Overview of money remittance in Belgium

Money transfers by all money remitters present in Belgium

(2019, yearly total, payment institutions established in Belgium or other EEA Member States)

Chart – Top-10 Country Corridors in value IN & OUT money transfer flows

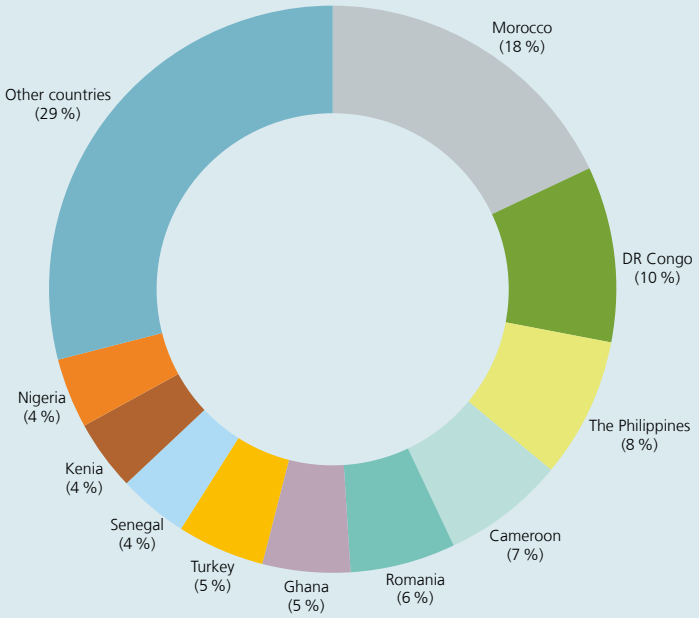


Overview of money remittance in Belgium

Money transfers by all money remitters present in Belgium

(2019, yearly total, payment institutions established in Belgium or other EEA Member States)

Chart – Top-10 Country Corridors in number of transactions IN & OUT money transfer flows



At the end of 2019, the total amount of incoming and outgoing money transfers via money remitters was € 1 546.8 million, an increase of 17.19 % and represented 5.798 million transactions, or an average amount of € 267 per transaction. Belgian payment institutions accounted for € 583.9 million, or 37.75 % against € 962.8 million of all EU money remitters active in Belgium and took a share of 42.89 % in the total of processed number of transactions in Belgium. The increase is due to the establishment of new institutions, mainly relocations of UK institutions in Belgium as a result of Brexit.

One current trend is the digitalisation of the money remittance business: nowadays, several remitters accept only digital pay inflows and try to pay out as much as possible cashless. As a result, the share of online remittance in Belgium, increased to 28.1 % in terms of value.

Taking into account both incoming (IN) and outgoing (OUT) money transfer flows, Morocco (18 %), the Democratic Republic of Congo (9 %), Turkey (8 %) and Romania (8 %) remain, like last year, the most important countries for the money remittance business taking place in Belgium in terms of value. The newly established money remitters in Belgium have had no significant influence on the importance of the different corridors for the time being although we observed increasing numbers of transactions with Cameroon and the Philippines compared to last year.

BOX 9

Brexit: impact on payment institutions

As was the case for CSDs and CCPs (see box 4), Brexit led to an end of passporting rights for UK payment and e-money institutions in Belgium on 1 January 2021. Belgian payment and e-money institutions that had passported into the UK prior to this date and registered for the temporary permissions regime for passporting EEA firms and investment funds (TPR) set up by the FCA are still able to keep their passporting rights on a temporary basis during a large part of 2021, provided they apply for authorisation in the United Kingdom.

The Bank granted licences to two further payment institutions with a Brexit background last year, namely Sendwave on 24 March 2020 and Jubilee Services on 25 February 2020. Since 2017, seven UK payment/electronic money institutions have been relocated to Belgium. Others may follow suit in the course of 2021.

3.3 Processors of payment transactions

Changes in regulatory framework

There were no changes in the Belgian regulatory framework during the period running from January to December 2020.

Prudential & oversight approach

In 2020, 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 equensWorldline SE as a systemically important processor of payment transactions performed through the Maestro card payment scheme (CPS) based on the data collected for the year 2019.

Table 3

List of systemically relevant payment processors

(as at 31 December 2020)

Systemically relevant payment processors	Payment scheme for which the legal threshold is exceeded	
	Bancontact	Maestro
Worldline NV/SA	✓	×
equensWorldline SE	✓	✓
Mastercard Europe SA	×	✓

Source: NBB.

Processors that qualify as being systemically important 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. Table 3 lists the processors of systemic importance and the schemes for which this status was notified.

Supervisory priorities in 2021

Regarding systemically important payment processors, the main focal point of the Bank will remain cyber resilience. (For Mastercard, see also the next section on card payment schemes.)

3.4 Card payment schemes

Regulatory framework

The regulatory framework devoted to card payment schemes (CPSs) remained unchanged in 2020.

In 2019 and 2020 the Eurosystem developed a new oversight framework for electronic payment instruments, schemes, and arrangements (PISA), a consolidation of existing frameworks in one over-arching set. This PISA framework based on the PFMI is intended to become the reference for Eurosystem oversight of payment instruments, schemes, and arrangements, thereby replacing the existing standards such as the "Harmonised oversight approach and oversight standards for payment instruments" (ECB, February 2009)[1] , the "Electronic money system security objectives" (ECB, May 2003), the "Oversight framework for card payment schemes – Standards" (ECB, January 2008)[2], the "Oversight framework for direct debit schemes" (ECB, October 2010)[3] and the "Oversight framework for credit transfer schemes" (ECB, October 2010)[4].

The PISA oversight framework aims at addressing recent regulatory changes (e.g. PSD2 and linked RTS and guidelines) and payment linked to technological developments. It can be considered as complementary to the existing oversight of payment systems and the prudential supervision of payment service providers. It includes an assessment methodology and an exemption policy. Schemes and arrangements of a certain importance and level of risk will be classified based on specific criteria relating to the size of the end user population, market penetration and geographic relevance and will have to comply with the requirements of the framework. The framework, assessment methodology and exemption policy have been submitted to a public consultation in November and December 2020[5] and are expected to be adopted in the course of 2021.

Oversight approach

In the euro area, the sound and safe functioning of card payment schemes is monitored by central bank oversight. The ECB, in cooperation with the Eurosystem national central banks, is in charge of the standard-setting process

1 Harmonised oversight approach and oversight standards for payment instruments (ECB, February 2009): https://www.ecb.europa.eu/pub/pdf/other/harmonisedoversightpaymentinstruments2009en.pdf.
2 Oversight framework for card payment schemes – Standards (ECB, January 2008): https://www.ecb.europa.eu/pub/pdf/other/oversightfwcardpaymentsss200801en.pdf.
3 Oversight framework for direct debit schemes (ECB, October 2010): https://www.ecb.europa.eu/pub/pdf/other/oversightframeworkdirectdebitschemes2010en.pdf.
4 Oversight framework for credit transfer schemes (ECB, October 2010): https://www.ecb.europa.eu/pub/pdf/other/oversightframeworkcredittransferschemes2010en.pdf.
5 Public consultation on the draft Eurosystem oversight framework for electronic payment instruments, schemes and arrangements (europa.eu). Available at https://www.ecb.europa.eu/paym/intro/cons/html/pisa_oversight_framework.en.html.

regarding 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 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 CPSs, 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.

Regarding MCE which qualifies both as a CPS and as a SIPS, the new PISA framework explicitly stipulates that it will take into consideration the results of every oversight duty performed under the monitoring of its continuous compliance, as a SIPS (see section 3.1), with the requirements of the SIPS Regulation.

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) to set up the cooperative mechanism for monitoring compliance with IFR Article 7.1.a. The Bank was formally designated by seven other NCAs as lead NCA in charge of the coordination of the 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, (b) completed its provisional analysis of its compliance with the so-called IFR and related RTS, and (c) shared its analysis with the cooperative working group members.

Oversight priorities in 2021

It remains to be established whether the assessment of MCE under the perspective of the Cyber Resilience Oversight Expectations for FMIs (CROE[1], which define the Eurosystem's expectations in terms of cyber resilience) is going to be triggered by mid-2021 or at another juncture. The CROE analysis would apply in practice to MCE with no distinction being made between its both qualifications as a SIPS and as a CPS. This decision will depend on the progress achieved in the assessment of MCE as a SIPS (which is a long-lasting duty *per se*).

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

1 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 domains which of the three maturity levels (Evolving, Advancing, Innovating) must be achieved by the systems according to their risk profiles and specific activities. The eight domains covered by the CROE are Governance, Identification, Protection, Detection, Response and Recovery, Testing, Situational Awareness and Learning and Evolving.

performed via a joint assessment group (JOT) under the coordination of the NBB and the ECB, consisting of participating Eurosystem NCBs.

After receipt and integration of the contributions from the members of the cooperative working group, and potential subsequent contributions from MCE, a final report, entitled "analysis of the compliance of MCE with IFR Article 7.1.a)" will be drafted by the end of the third quarter of 2021. As a reminder, this part of the IFR for which the Bank acts as lead NCA does concern the monitoring of the effective separation between scheme and processing activities under the perspective of the accounting, organisation and decision-making processes.

Regarding the IFR cooperation mechanism for ensuring compliance of MCE with IFR Article 7.1.a, the assessment exercise, performed by the whole cooperative working group, is expected to be finalised by the third quarter of 2021.

The next step regarding oversight of Bancontact as a CPS will be an assessment based on the new PISA framework. It should be conducted in the context of a Eurosystem-wide exercise to be decided after the finalisation of the PISA Framework.

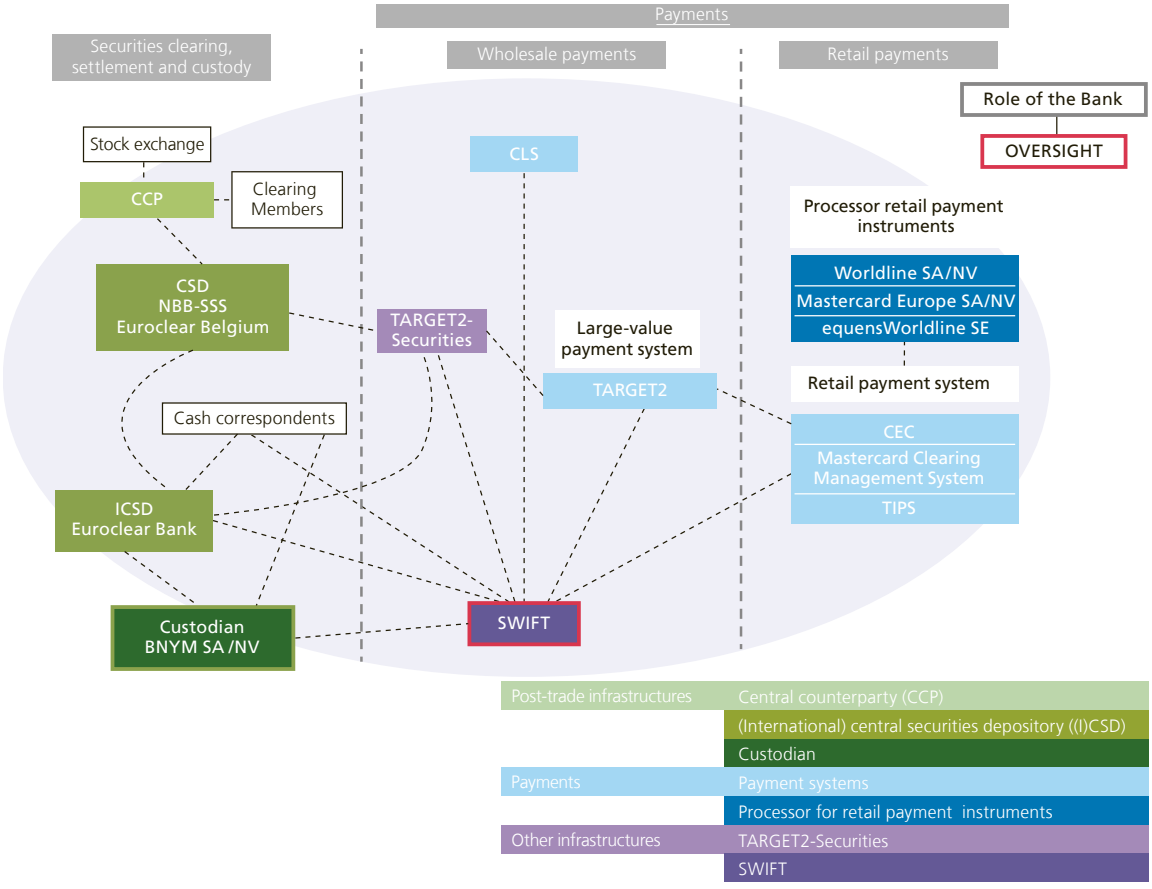
4. SWIFT

The Society for Worldwide Interbank Financial Telecommunication (SWIFT) provides global messaging and connectivity services to various financial institutions and market infrastructures, such as banks, brokers, investment managers and other. SWIFT is a limited liability cooperative company registered in Belgium and has its headquarters in La Hulpe.

Correspondent banking activities and financial market infrastructures systemically depend on SWIFT for its financial messaging. SWIFT thus plays a fundamental role in the global financial industry and acts as a critical service provider to the financial institutions and market infrastructures (see chart 4). For this reason, the G10 central banks have classified SWIFT as systemically vital and established the cooperative central bank oversight on SWIFT.

Chart 4

SWIFT as a critical service provider to the financial industry



4.1 Oversight approach

At the end of 1997, a formal set-up of the oversight on SWIFT was established by the G10 central banks[1]. At the heart of this formalised structure lies the international cooperative arrangement conducted by the G10 with the objective of overseeing the adequate and safe functioning of SWIFT. Since SWIFT is based in Belgium, the National Bank of Belgium holds the mandate of lead overseer and chairs the international oversight meetings.

International dimension

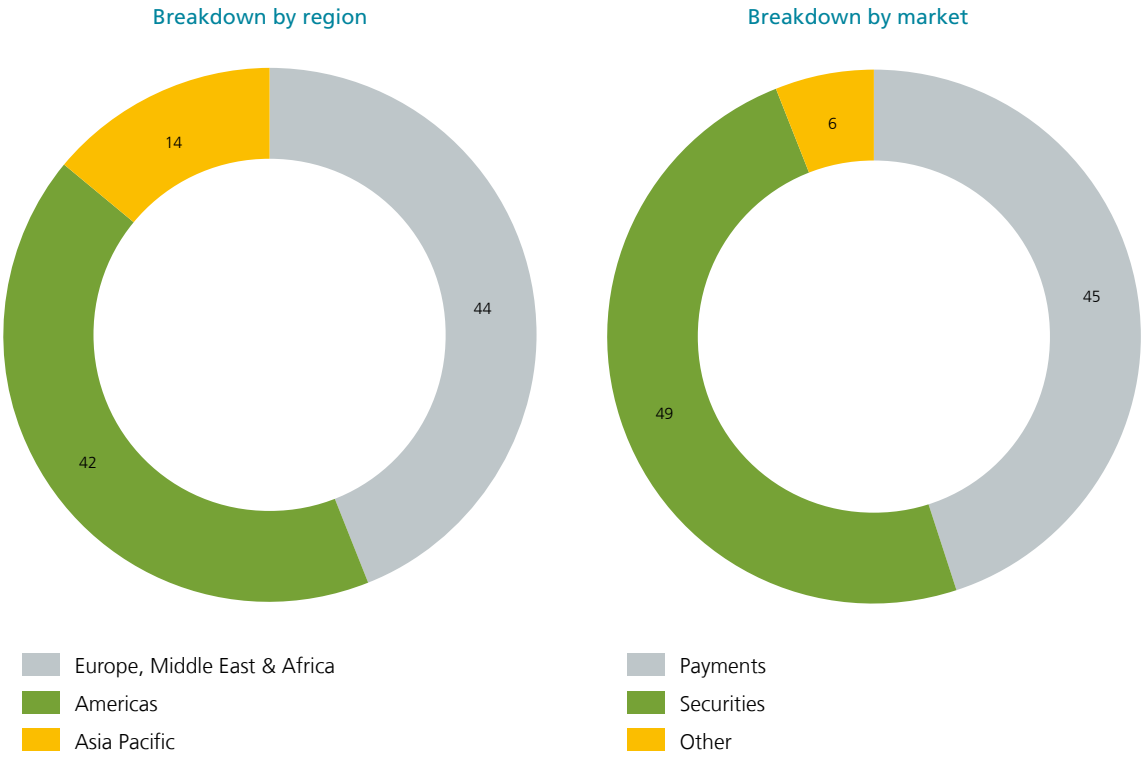
SWIFT operates in an international context with activities spread over more than 200 nations. This is illustrated by the company's messaging volumes: in 2020 9.5 billion messages (+10.3 % compared to 2019) were sent with an average of 37.7 million messages per day.

SWIFT is owned and controlled by its users, who are organised in national member groups, user groups and dedicated work groups. It arranges frequent touchpoints with these different parties to ensure continuous dialogue and timely updates on strategy or product developments. The industry-specific work groups cover various topics for discussion between SWIFT and its users, for example security hardenings of its interfaces, new

1 The G10 central banks involved in the SWIFT oversight are 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.

Chart 5

SWIFT FIN activity



Source: SWIFT.

technology implementations, messaging service changes. An example of such a dedicated work group is the Payments Market Practice Group[1].

The message traffic over SWIFT's network determines the company's share distribution. As a result, the shares are reallocated every three years in order to more realistically mirror the SWIFT messaging user community. SWIFT Board members are appointed by the countries or country constituencies based on the number of shares owned by all users in the respective jurisdiction. The previous redistribution took place in 2018, which means that one will take place during this year's annual general meeting. The next share revision is scheduled for 2024.

SWIFT's FIN traffic for 2020 per market and region is illustrated by the following two charts. FIN is SWIFT's core messaging service for sending and receiving financial messages. There are 11 588 live users of whom 2 372 represent shareholders. As in previous years, the 2020 payments (45 %) and securities (49 %) messaging represent the largest categories. The Europe, Middle East & Africa region has the largest share (44 %) of the total 2020 FIN traffic volume.

International cooperative arrangement

The central banks that roughly represent the G20 countries[2] are directly involved in the international cooperative oversight of SWIFT. This arrangement is formalised in a framework which sets out the role of the NBB as lead overseer, and the scope and frequency of the different oversight work groups.

The NBB's role as lead overseer consists of the daily monitoring and follow-up of SWIFT's activities and projects. Depending on the topic, frequent bilateral interactions take place between SWIFT's three lines of defence[3] and the NBB oversight team. The information relevant to the other overseers is shared in order to ensure a transparent cooperative oversight with the other central banks. The relationship between SWIFT and the NBB is defined via the SWIFT Oversight Protocol. The NBB also integrates another main activity in its mandate as lead overseer, namely the coordination and organisation of the different international workgroups it chairs. In that capacity, the NBB oversight team also drives the SWIFT oversight outreach activities to other stakeholders, such as the central banks that are not directly involved in these oversight activities.

There are four work groups defined in the oversight framework : Cooperative Oversight Group (OG), Executive Group (EG), Technical Group (TG) and SWIFT Oversight Forum (SOF). Each group has a specified scope and frequency of interaction. In addition, touchpoints exist between the different groups and with SWIFT. The SWIFT oversight relationships between the SWIFT overseers and the NBB are laid down in a Memorandum of Understanding (MoU). The following paragraphs provide more detail on the different oversight bodies.

The Cooperative Oversight Group (OG) is represented by the G10 central banks and the chairperson of the CPMI. Each G10 central bank appoints a senior-level overseer to participate in the two annual meetings. OG members decide on SWIFT oversight planning, conclusions, policies and recommendations to SWIFT. Throughout the year, there are also *ad-hoc* interactions scheduled with the OG members when certain developments at SWIFT require additional review.

The OG decisions and recommendations are communicated to SWIFT in the Executive Group (EG) meetings that typically take place after the OG meeting and after a SWIFT Board meeting. Each year, three EG meetings take place in order to better align with the OG meetings and to ensure SWIFT shares information with overseers on SWIFT Board decisions and developments in good time. The EG consists of a sub-set of the OG members which

1 SWIFT established the Payments Market Practice Group (PMPG) to facilitate the ISO 20022 global migration. The PMPG consists of market infrastructure and bank representatives.

2 The G20 countries directly involved in SWIFT oversight are represented by the G10 central banks 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).

3 The three lines of defence traditionally represent the first line that owns and manages risk, the second line that oversees and challenges the first line's risk management, and the third line that is responsible for independent assurance.

represent the four major global currencies, i.e. NBB as chair, Bank of Japan, Bank of England, European Central Bank, and Federal Reserve Board of Governors. Overseers communicate the OG decisions and recommendations directly to the SWIFT delegation, consisting of the SWIFT Executive Management and Board members.

The G10 Technical Group (TG) conducts the technical fieldwork of SWIFT developments and projects, and reports directly to the OG. Four meetings are planned each year, which include foreseen interactions with SWIFT management, internal audit and independent risk functions in order to carry out the deeper technical oversight analysis. Skills and knowledge on technological and IT-specific domains are required to better understand these developments and their accompanying risks within SWIFT.

The SWIFT Oversight Forum (SOF) represents a wider group of countries based on their share in the total SWIFT traffic volume and in alignment with the CPMI membership composition. The SOF consists of the G10 OG senior-level overseers 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). The SWIFT oversight conclusions, planning and priorities are shared with the SOF. Furthermore, the SOF provides input to OG discussions and serves as a platform for communication on system interdependencies related to the use of SWIFT in their jurisdictions. The NBB continuously seeks ways to improve its outreach to other central banks, as is depicted in the following box.

BOX 10

Involving the central bank community

SWIFT's critical and systemic nature to the financial industry and the 2018 IMF recommendations to further extend the sharing of oversight information to the wider central bank community resulted in the strengthened involvement of the SOF and in the organisation of outreach activities.

In 2012, the G10 Technical Group (TG), Oversight Group (OG) and Executive Group (EG) were supplemented with the SWIFT Oversight Forum (SOF). The SOF enables information-sharing on SWIFT oversight activities with a wider group of central banks. In line with the expansion of the Committee on Payments and Market Infrastructures (CPMI), new members were invited to join the SOF in 2019: Argentina, Indonesia and Spain. At the same time, pending invitations for Brazil and Mexico were updated.

The key objectives as specified in the SOF Terms of Reference are the following:

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

With the aim of continuously widening information-sharing, it has been decided to involve the SOF members more actively in Customer Security Programme (CSP) topics. A larger number of central banks

play an important role to reach out on CSP either to other authorities (e.g. bank supervisors) or to other jurisdictions beyond the SOF countries or through regional outreach initiatives.

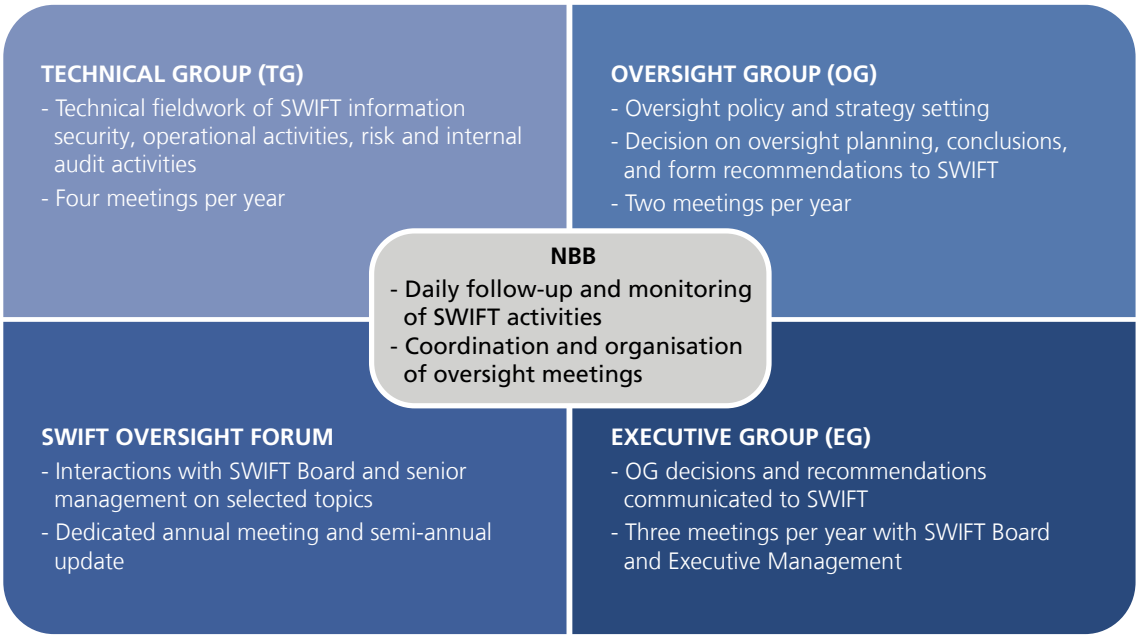
The NBB has organised such regional initiatives on previous occasions. The first regional outreach session took place in 2018 during SWIFT's Sibos conference. The aim was to interact and engage with both the directly involved SWIFT overseers and the non-G20 central bankers on SWIFT oversight topics, such as oversight conclusions, priorities, major SWIFT developments, possible impact on users, and the importance of the role of the SWIFT community. Such outreach sessions during SWIFT's international conference have multiple advantages : a large and globally widespread delegation attends Sibos, each year Sibos is located in another continent, and the majority of the Sibos participants are senior central bank representatives and directors of payments, IT and FMI oversight departments. The second outreach session took place during the 2019 Sibos event, attracting about 70 participants from more than 50 different countries.

A third regional outreach session was planned during the 2020 Sibos conference. Unfortunately, this had to be cancelled because of the COVID-19 pandemic outbreak. SWIFT re-arranged its physical event into a digital Sibos, which made it impractical to organise the foreseen oversight outreach session.

As one of the standing SOF members, the Monetary Authority of Singapore and the NBB planned to jointly hold an outreach session in February 2020 to interact with central banks and supervisory authorities from South-East Asia on relevant SWIFT oversight activities. However, this planned meeting also had to be postponed as a result of the global pandemic but will be rescheduled when circumstances allow.

The following figure gives an overview of the different workgroups involved in the SWIFT oversight.

Cooperative Oversight of SWIFT through different international workgroups



The work group organisations mentioned in the above figure had to be reshuffled because of COVID-19. The planned physical meetings in 2020 were switched to multiple virtual meetings in order to execute and finalise the foreseen planning of oversight activities. The next box provides more information as to what extent COVID-19 impacted SWIFT's oversight work.

BOX 11

COVID-19 impact on oversight activities

The COVID-19 virus spread globally in a sudden and unexpected manner. Therefore, overseers had to logistically rearrange their SWIFT oversight activities. Traditionally, multiple physical meetings with the other central bank overseers are organised throughout the year. The crisis situation forced authorities to restrict travelling, which led to the cancellation of physical oversight and outreach meetings. Nevertheless, the overseers continued their critical review on SWIFT in a decentralised manner in order to cover planned areas such as cyber security, Enterprise Risk Management, Customer Security Programme, and Internal Audit topics. In addition, the COVID-19 implications for SWIFT became a recurring topic for discussion and analysis in the different workgroups.

The OG, EG, TG and SOF meetings all took place virtually in 2020. The four TG meetings were replaced by a series of conference calls aligned with the initially foreseen 2020 oversight planning. As it became clear that the COVID-19 situation would persist until at least the end of 2020 with generalised working from home, the TG refocused its activities around three main guiding principles:

- operational risks, both general and pandemic-related, require close monitoring (e.g. cybersecurity strategy):
- critical business, technology and IT projects must be reviewed (e.g. ISO 20022 migration):
- assurance on the effectiveness of the three lines of defence needs to be obtained.

On top of the conference calls and as a standard work practice, the TG also analysed the extensive documents provided by SWIFT. Follow-up items were identified and communicated over written procedure and conference calls.

On-site reviews have been recently added to the SWIFT oversight toolbox in order to gain additional and deeper knowledge on certain SWIFT domains for which the current oversight structure foresees limited possibilities. In 2018, an extensive on-site review took place on SWIFT's Enterprise Risk Management. In view of the insight gained, the overseers decided to organise a second review in 2020 on cyber security. The initially planned review in the first quarter of 2020 had to be postponed owing to visitor restrictions at SWIFT imposed at the beginning of the pandemic, international travel restrictions and other uncertainties. Eventually, the on-site review team decided to carry out the scheduled review on cyber security through a decentralised approach. Instead of the physical interactions with SWIFT, the review took place over a series of virtual meetings at the end of 2020 to finalise the foreseen activities.

Thanks to the possibility of organising the SWIFT oversight meetings digitally, the pandemic generally did not blur the 2020 oversight priorities and overseers continued to adequately assess SWIFT's activities from a cyber and operational risk-based view.

Oversight expectations

SWIFT oversight risk-based activities are focused around the five High-Level Expectations (HLEs): (i) Risk Identification and Management, (ii) Information Security, (iii) Reliability and Resilience, (iv) Technology Planning, and (v) Communication with Users. Through these expectations, overseers assess SWIFT's adequacy of managing operational and technology risks. The HLEs form the basis for the oversight planning, discussions and priority setting. These 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 be in accordance with the five HLEs. This is assessed through different channels: bilateral discussions between NBB and SWIFT, frequent TG interactions with SWIFT's three lines of defence, interactions with SWIFT senior management at OG and SOF meetings, interactions with SWIFT Board and senior management at EG meetings, and through analysing documentation provided by SWIFT. SWIFT's reporting to overseers serves as input for oversight follow-up and gives also an indication of the risk drivers for SWIFT. Standing topics in the oversight analysis are ERM, information security, technology implementation and risk management.

4.2 Covered oversight topics in 2020

Overseers seek to obtain assurance that the corresponding risks in the domains as listed in the five HLEs are adequately assessed, monitored and mitigated in contemplation of the reliability of SWIFT's services. An important topic for overseers is the SWIFT Customer Security Programme (CSP), which received extensive attention from overseers in 2020. Other major projects, such as the planned ISO 20022 migration for cross-border payments and cash management have been included in the overseers' review. The COVID-19 pandemic implied an additional oversight attention point. Overseers assessed its impact on SWIFT's projects, operations, security and resilience, and also the adequacy of SWIFT's response and mitigating actions to the new emerging risks and challenges caused by the pandemic.

Customer Security Programme (CSP)

Since the cyber threat to the financial industry has not diminished, overseers continued to review the effectiveness and further maturing of the CSP in 2020. In the aftermath of the 2016 Bangladesh cyber heist, SWIFT launched the CSP. Through this Programme, SWIFT endeavours to enhance the cyber security in its user community and wider financial industry against potential hackers. The CSP sets out certain requirements how users are expected to adequately secure their on-premise IT components that connect to SWIFT's secure network.

The Customer Security Control Framework (CSCF) has been analysed by overseers on the effectiveness of the implementation and reporting processes. The CSCF consists of a set of mandatory and advisory controls. SWIFT users are expected to be compliant with the mandatory security controls which set a security baseline. The advisory controls are also applicable to all SWIFT users but describe rather good practices for securing local IT infrastructures. A SWIFT user is encouraged to also be in accordance with these advisory controls. A user's compliance is reported through a self-attestation to the framework, which is uploaded through SWIFT's Know Your Customer – Self Attestation (KYC-SA) tool by the end of each year.

By 31 December 2020, 89 % of customers had submitted their attestation for the mandatory controls. The number of self-attestations for 2020 shows a similar uptake compared to 2019. SWIFT provides overseers with quality assurance and monthly metrics reports, which contain an overview of the attestation levels, consultation, reporting processes' effectiveness, and the security advances across different user types. Overseers actively analyse these reports provided by SWIFT. In order to improve the monitoring capabilities, overseers assume SWIFT will refine and extend the CSP reporting metrics. In 2020, a dedicated CSP working group had been temporarily

established with overseers and SWIFT representatives to carry out an in-depth review as to how SWIFT could better meet overseers' expectations on CSP reporting.

Each year, SWIFT publishes a new version of its CSCF. In 2020, it prepared CSCF v2021 which was published in mid-2020 and with which users are expected to be compliant with by the end of 2021. Before SWIFT formally implements the new framework version, a consultation process is planned which involves two main external stakeholders: the user community and SWIFT overseers. For the user community, SWIFT collects feedback through the National Member Groups. As second main stakeholder in the yearly recurring consultation process, overseers have the possibility to provide input to SWIFT's suggested CSCF version adaptations of mandatory and advisory controls. Other stakeholders involved in the consultation process are cyber security experts and supervisory authorities. To reduce the operational burden on its participants in context of the pandemic, SWIFT included limited changes in CSCF v2021: one advisory control, which was part of a mandatory control in previous framework versions, was promoted to mandatory. Multiple existing controls received clarifications on their implementation.

In 2020, overseers also followed up on the enhanced role for supervisory authorities, more specifically on SWIFT's initiatives to onboard supervisors to SWIFT's Know-Your-Supervisor (KYS) tool. Through the KYS tool, supervisors will be able to retrieve self-attestation data of financial institutions in their jurisdiction. The self-attestation information could serve as an important input for risk-based planning and scoping for supervisory authorities. SWIFT reserves the right to report to the competent supervisory authorities those users who have failed to self-attest full compliance with all mandatory CSCF controls in time or users who depend on non-compliant service providers.

The requirement for all SWIFT users to complement their self-attestations with an independent assessment conducted by internal or external auditors was initially planned to kick off in 2020, but the pandemic complicated implementation (e.g. restricted physical inspections). After the overseers' review, SWIFT ultimately decided to postpone the launch of the Independent Assessment Framework, as part of its mitigating CSP actions. The box on "mitigating initiatives taken by SWIFT" in the next paragraph on COVID-19 highlights the CSP and other mitigating initiatives SWIFT considered as a result of the crisis.

The consultation process, in which a user has the possibility of using information from their counterparties' CSCF self-attestations, was also followed up by overseers in 2020. SWIFT proposed improvements to this process to stimulate peer pressure of improving a user's counterparties' risk-mitigating measures and security position. SWIFT further enhanced the KYC-SA functionality to ensure that counterparties have access to more actionable information and smoothened the consultation functionalities. Overseers will continue their review on this process and SWIFT's proposed improvements.

Overseers also include in their annual CSP analysis the monitoring of SWIFT's fraud and detection tools, such as the Sanction Screening Service, which screens financial messages against international sanction lists before sending it through SWIFT's network, and the Payment Control Service, which filters a message against certain user-set rules before the message can be processed. SWIFT offers various tools to prevent and detect fraud incidents to help its users combat fraudulent payments and strengthen their existing security measures. Overseers include the effectiveness and enhancements of such SWIFT tools in their annual review. This is in line with the CPMI's strategy for reducing the risk of wholesale payments fraud related to endpoint security.

In 2020, overseers assessed the transparency and rigour of SWIFT's communication processes to its users in the event of technology changes, fraudulent compromises, and updates on common fraud practices in the industry. The CSP dedicates information-sharing as one of its foundational pillars supporting its users to adequately improve their incident and risk management processes. SWIFT's Information Sharing and Analysis Centre (ISAC) provides users with actionable business knowledge on cyber threats, indicators of compromise, and used hackers' techniques, tools and procedures. SWIFT targets both technical and business professionals through its ISAC portal facilitating a digestible format for information-sharing.

Cyber attacks targeting SWIFT participants have continued over the course of 2020, which are not expected to slow down. Overseers obtaining reasonable assurance on the effectiveness of the CSP and its features benefits the overall financial community in terms of reducing fraudulent transactions as a result of cyber hacks. The oversight objective remains to ensure that the security requirements evolve in line with new threats, improvements in cyber security capabilities and regulatory expectations.

COVID-19

Since the functioning of the financial sector heavily relies on SWIFT's core messaging services, overseers closely followed up on SWIFT's responsibility to ensure its operations as critical infrastructure during the materialised extreme scenario of a worldwide pandemic outbreak. Therefore in 2020, the COVID-19 impact on SWIFT, the company's response to it and implementation of mitigating actions became a standing topic under overseers' review activities. They conducted such analysis based on frequent written statements provided by SWIFT and multiple interactions with members of the Executive Management on SWIFT's security status and risk monitoring.

Like many other international organisations, SWIFT had to adapt and react to the impact of COVID-19. SWIFT began early monitoring of the situation in accordance with national and local authorities' measures. Given its role as critical service provider, SWIFT's main priority was to safeguard the operationality and availability of its critical messaging infrastructure avoiding any global interruption. Despite the closure of multiple offices, SWIFT has been able to ensure business continuity of its services thanks to generalised working from home for its employees, and the reorganisation of staff being able to work at the necessary SWIFT locations.

To lower the burden on its customers, SWIFT implemented several mitigating measures, which are further detailed in the box below.

BOX 12

Mitigating initiatives taken by SWIFT

In order to reduce the operational burden on its users in context of the pandemic and generalised working from home, SWIFT decided to implement multiple mitigating actions regarding the Customer Security Programme (CSP), and the yearly Standards Release. Before SWIFT had implemented the mitigations, overseers sought assurance in their analysis that these would not cause any drawbacks to the targeted CSP security objectives in the SWIFT user community.

SWIFT implemented the following CSP mitigations:

- For 2020, customers needed to re-attest against the existing set of CSCF v2019 controls by December 2020. The updated CSCF v2021 will come into effect in July 2021, with the normal year-end deadline for compliance. The CSCF v2021 includes a promoted advisory control to mandatory regarding the restriction of internet access in the IT infrastructure in the user environment that connects to the SWIFT network.
- The independent assessment for self-attestations (i.e. the requirement to get an opinion of the accuracy of the self-attestation from either an independent internal assessor or an external third-party assessor) will be aligned with the CSCF v2021.
- The next round of sampled mandatory external assessments will also be launched in line with the CSCF v2021.

A second mitigating action consisted of a scope reduction of the 2020 Standards Release. SWIFT decided to prioritise the standard changes for the securities messages. All initially planned other changes for 2020 have been postponed to November 2021. The 2021 Standards Release will include the 2020 changes (excluding the securities' standard changes) and agreed 2021 changes.

For 2021, overseers expect the adoption of the independent assurance framework and the resumption of mandated external audits and will review their outcomes.

Other topics

In addition to the overseers' considerable attention on CSP and the COVID-19 impact on SWIFT, the overall focal point remains on the security and availability of SWIFT's activities and core messaging services at any given time or circumstance.

Overseers' yearly activities are based around the five High-Level Expectations (HLEs).

For the first HLE "Risk Identification and Management", overseers assess SWIFT's Enterprise Risk Management (ERM) and audit activities. Included in this review are the effectiveness and independence of these lines of defence, and their interactions with each other. Overseers have revised the further maturing of SWIFT's risk management practices and how the second line of defence coped with the impact of the pandemic on SWIFT on the short and longer term. It was and still is important that SWIFT achieves the most critical project objectives, even during a crisis. The functioning and control work of SWIFT's auditors has been challenged by overseers with continuous analysis on their provided opinions and findings. Frequent interactions with SWIFT's Chief Risk Officer and Chief Auditor have given better insight into these above-mentioned topics.

Cyber security, which falls under the second HLE "Information Security", remains a major priority for overseers. Each year, there is a thorough analysis of SWIFT's proposed cyber security strategy and security roadmap activities. Overseers expect that SWIFT foresees the necessary investment and maintains the maturity of key security capabilities to safeguard the functioning of its critical messaging services. The evaluation of the design, implementation and improvement of cyber detection, response and recovery capabilities contributes to obtain such assurance. As a sequel to the first in-depth on-site review on ERM in 2018, a second on-site review took place virtually in 2020 on SWIFT's cyber security, which has not been finalised yet. A second large pillar of HLE 2 is the CSP, which is described in paragraph "Customer Security Programme" above.

Incidents and business continuity are vested in HLE 3 "Reliability and Resilience". Overseers investigate incidents that disrupt SWIFT's services. For each incident, SWIFT shares with the overseers the sequence of the incident events, impact on its users, and action plan to avoid similar incidents in the future. Overseers share their expectations to SWIFT on the incident management processes so that this critical communication continues to be refined. Considering the pandemic, the precautionary and responsive measures that SWIFT undertook to maintain business continuity have also been included in the oversight discussions.

For HLE 4 "Technology Planning", overseers closely follow up on the impact of new technologies and processes on the entire SWIFT organisation and its community. In 2020, SWIFT launched its new strategy in which there

will be a shift of the current sequential messaging to end-to-end transactions. This change will be aligned with the ISO 2002[2] migration of cross-border payments and cash management. In this approach, SWIFT envisages that users will be able adopt the ISO 20022 format at their own pace. SWIFT's new strategy reorientation was often put on the agenda in the course of 2020 to better grasp the alignment between its business and IT strategies, more specifically the project development steps, milestones and interaction with customers. This will be continued in 2021.

During 2020, overseers organised a deep dive on HLE 5 "Communication with Users". The objective for this session was to have a first dedicated interaction with SWIFT's recently appointed Chief Customer Experience Officer. The deep dive provided overseers with insight into the objectives of SWIFT's communication with customers and the processes to ensure care across all customer touchpoints. This will become ever more important for the further roll-out of SWIFT's new strategy course and ISO 20022 migration start in 2022. Overseers are keen on analysing the coming developments.

4.3 Oversight priorities in 2021

Overseers follow a risk-based approach for the yearly planning of SWIFT oversight activities. Each quarter, they evaluate the covered topics and use this information to identify which items or domains require additional critical review or which new topics need to be included in future analysis. Thanks to this method, overseers have the flexibility to add items or change the review frequency of certain topics, which contributes to the continuous oversight format throughout the entire year.

In 2021, the changing environment in which SWIFT operates and the company's anticipation of such changes will be on the agenda. More specifically, the focus remains on the adequacy of SWIFT's cyber management and strategy to cope with the ever-evolving cyber threat. Part of the analysis includes the review on SWIFT's cyber security roadmap and corresponding investment plan. Each year, overseers also challenge the provided ISAE 3000 reports of SWIFT's external security auditor.

Technological changes and their impact on SWIFT will also be one of the top oversight priorities in 2021. Overseers will continue to seek assurance that the corresponding risks in these domains are adequately assessed, managed, and mitigated for SWIFT to ensure business continuity of its services.

Another oversight top priority remains the different components of the CSP. A sub-set of certain follow-up CSP items include the following: CSCF control framework consultation process and its effectiveness, refinement of existing and additional CSP metrics, compliance levels of SWIFT's community against the mandatory and advisory security controls, further maturing of supervisory authorities' involvement, outreach to relevant stakeholders, outcomes of the mandatory independent assessments.

On top of these areas, a fourth major category covers standing topics, such as interactions with SWIFT's risk department, review of internal audit reports, follow-up of incidents and associated action plans, operational resilience activities and other.

The five HLEs lie at the heart of the overall oversight analysis work and planning. These HLEs form the starting point of identifying the topics to cover annually from a risk-based perspective. Since there is an extensive set of topics to be covered by overseers each year, the following items are a shortlisted indication of topics that will be included in 2021:

- HLE 1 Risk Identification and Management:
  - SWIFT's overall risk profile and topic-specific risk assessments;
  - internal and external audit findings, and identified mitigations that management undertakes.

- HLE 2 Information Security:
  - Customer Security Programme KYS functionality;
  - attack vectors of logical intrusion tests.
- HLE 3 Reliability and Resilience:
  - business continuity management enhancement;
  - impact of technological evolutions on SWIFT's resilience.
- HLE 4 Technology Planning:
  - changes in technology risk on existing IT infrastructure;
  - platform that facilitates ISO 20022 transactions.
- HLE 5 Communication with Users:
  - SWIFT's communication on ISO 20022 migration towards customers;
  - customer experience roadmap.

Specific thematic articles

Activities of Big Tech companies, international payment card schemes and European initiatives

Jan Vermeulen

The retail payments ecosystem is constantly evolving and, over the last decade, has gone through important changes such as the entry of major, global technology companies. Those international/global players and large technology players are perceived to potentially endanger the European strategic autonomy for payments-related issues. They have started to offer regulated payment services in the European Union and obtained licences to offer payment services from different home countries, with the possibility of passporting their activities in the rest of the European Economic Area (EEA). Google[1], Amazon[2] and Facebook[3] have an electronic money institution licence in, respectively, Lithuania, Luxemburg and Ireland. Paypal[4] has a credit institution licence in Luxemburg.

Among the large companies active in the field of payments in Europe, two groups can be distinguished according to the nature of their activities. These are, on the one hand, the new players often referred to as GAFA[5] and, on the other hand, the more traditional players such as international card payment schemes by VISA and Mastercard. Since a few years, European regulators and market actors (separately or together) take initiatives to foster genuine European payment solution initiatives.

GAFA

With the exception of Facebook's Diem (formerly Libra) stablecoin project, GAFA are not creating any new payment instruments or schemes. They engage in payment services to improve or expand their ecosystems. This usually involves integrating existing payment instruments/methods by offering a new method to initiate payments in a simpler and/or more secure way for users. They offer complementary services to existing payment services, generally at the level of payment initiation, most often by partnering with traditional players such as card issuers (banks) and acquirers. Their services are predominantly based on the existing infrastructures of international payment cards. Among the main payment services offered in Europe by GAFA, we find:

1 Google Payment Lithuania UAB.
2 Amazon Payments Europe S.C.A.
3 Facebook Payments International Limited.
4 PayPal (Europe) S.a r.l. et Cie, S.C.A.
5 Google, Apple, Facebook, Amazon.

AmazonPay: is a service offered by Amazon to allow holders of an Amazon account to use payment methods registered therein to pay at other merchants, outside the Amazon platform, affiliated with this service. With AmazonPay, customers therefore do not have to open a specific account with each merchant. In Belgium, this service is offered in cooperation with the purchaser Adyen. In most cases, payments made through AmazonPay are card payments based on international schemes.

GooglePay and ApplePay: are "wallets" specific to the Google and Apple ecosystem, making it possible to digitise participating credit and debit cards (mainly Visa, Mastercard and Maestro in Europe) and to make payments more securely by linking the card to the smartphone on which the application is located and without communicating the card information during a payment (they are replaced by a "token" whose usage is limited).

Facebook's Diem project sets itself apart from the payment services traditionally set up by GAFA in that it was about to create a form of international crypto-currency. This project provoked an outcry from regulators around the world and was scaled down to a US pilot project with a USD-only backed crypto-asset. The European Commission's Digital Finance Package proposal includes a draft Regulation intended to regulate this type of instrument (Proposal for a Regulation of Markets in Crypto-Assets or MiCA, see thematic article).

International card payment schemes Visa and Mastercard

The Visa and Mastercard schemes unquestionably dominate the European card payment market. Only a few domestic schemes remain, as is the case in Belgium for Bancontact. To counter competition with the international schemes, six national schemes (including Bancontact) set up the European Card Payment Cooperation (ECPC) in 2020, whose objective is to offer alternatives to the VISA and MasterCard specifications for EMV cards and contactless kernels of terminals.

European market, policy and regulatory initiatives

Europe is currently the only major economy that does not have its own regional POS/ecommerce payment solution and is totally dependent on international schemes for cross border payments. By defining a retail payments strategy (see box 6), the European Commission is determined to change this situation, in particular with the European Payments Initiative which aims to develop a genuine pan-European payment solution.

Other initiatives on various topics are being taken:

The European Payments Initiative: The European Payments Initiative, or EPI, is a payments integration initiative set up by the European banking sector[1] in response to a call from the ECB for the creation of a payments system and a pan-European interbank network capable of competing with international schemes. The project has received support from the European Commission and the ECB.

SEPA Request To Pay scheme (SRTP): The SRTP scheme covers the set of operating rules and technical elements (including messages) that allow a payee to request the initiation of a payment from a payer in a wide range of physical or online use cases. It was developed by the European Payments Council (EPC) and may be used in the context of the EPI.

1 KBC Bank is one of the participating members.

European Digital Payments Industry Alliance (EDPIA) is an alliance founded by five large European payment services providers (Worldline, Nets, SIA, Ingenico and Nexi). It intends to represent the interests of independent payment services providers headquartered in Europe, non-banked owned, and its purpose is to contribute to EU policy debates that define the business environment for electronic payments, and to strengthen the visibility and understanding of the European payments industry. The Alliance focuses on the "acquiring functions" perspective.

Another initiative is the **European Mobile Payment Systems Association** (EMPSA), twelve mobile payment systems (of which Bancontact Payconiq Company) trying to enable interoperability both on the technical and commercial/business level with a view of seamless mobile payment across Europe.

The Eurosystem oversight framework for electronic payment instruments schemes and arrangements (PISA framework) establishes oversight requirements in the form of generic principles to assess the safety and efficiency of the entities that fall within the scope of its oversight and to induce change where shortcomings are identified. The PISA framework sets out those oversight principles in a single, future-proof and harmonised manner for electronic payment instruments, schemes and arrangements.

Market contact groups

- The Advisory Group on Market Infrastructures for Payments (AMI-Pay) is a forum that assists the Eurosystem in fostering payment innovation and integration across Europe and offers advice on the provision and modification of Eurosystem payment-related services. It is composed of banks active in the European Union and of national central banks.

- The European Retail Payments Board (ERPB) was set up to foster the development of an integrated, innovative and competitive market for retail payments in euro in the European Union. The group consists of all stakeholders in the payment ecosystem: regulators, payment service providers, retailers, enterprises and public administrations.

Markets in Crypto-Assets

Axel Van Genechten

The advent of digital currencies has spurred global regulators into action in recent years, leading to growing debate on central bank digital currencies[1], increasing regulation, a plethora of reports pondering the various threats and opportunities these currencies create, and considerable questions regarding the role of the State and monetary sovereignty in the 21st century. As part of its Digital Finance Package, the European Commission released its own legislative proposal concerning crypto-assets on 22 September 2020. The proposed framework, commonly referred to as the Markets in Crypto-Assets Regulation[2] or MiCA, aims to support innovation within EU financial markets while upholding standards concerning consumer protection, market integrity, financial stability, monetary policy transmission, and monetary sovereignty. Primarily aimed at crypto-currency service providers and so-called stablecoins, the proposal seeks to balance the need for legal certainty with the limited efficacy of regulating highly mobile assets in a globalised, digital world.

Crypto-assets

Crypto-currency is often described as a digital or virtual currency that relies on cryptography to prove ownership and protect the integrity of transaction records. The typical use of a decentralised governance model, whereby control is distributed away from a central authority, is one of the aspects that sets it apart from more traditional e-money. The infrastructure supporting this model is called distributed ledger technology (DLT), often in the form of a blockchain. Since the launch of Bitcoin in 2009, crypto-currencies have really taken off across the world in various forms with a market cap reportedly exceeding $ 1 trillion[3] in 2021.

As an increasing number of asset managers and financial institutions are now willing to develop or invest in crypto-assets, which may result in a prominent role for this asset class in the future. Macro-economic developments such as global monetary and fiscal policy, as well as rising government debt are suspected of fuelling this rise by some analysts, with some investment banks speculating that crypto-currency could even take the place of gold as the favoured hedge against inflation by sceptics, or perhaps even gain the coveted status of world reserve currency[4].

Attempting to circumvent the volatility often seen in traditional crypto-currencies such as Bitcoin, stablecoins in particular could be more likely to grow into a global currency with widespread use. While anonymity and lack of

1 See next thematic article "Analysing a digital euro – A status update".

2 Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-Assets, and amending Directive (EU) 2019/1937.

3 According to data released by CoinGecko and reported in various media outlets.

4 Ruchir Sharma, global chief strategist for Morgan Stanley, FT opinion piece: https://www.ft.com/content/ea33b688-12e0-459c-80c5-2efba58e6f1a.

data preclude any definitive causes or explanations, the mere possibility of attaining economic prominence, and the risks this entails, among financial institutions and consumers forms an adequate impetus for regulators to step in.

MiCA casts a wide net in terms of definition of crypto-assets in its current form, defining these as *a digital representation of value or rights which may be transferred and stored electronically, using distributed ledger technology or similar technology*. While the draft Regulation covers any crypto-assets that are not yet regulated by other legislative instruments, the main focus of the proposal is on stablecoins. Noting the impossibility ofguaranteeing a truly stable value, the proposal splits these into categories based on the underlying assets: electronic money tokens (EMTs) and asset-referenced tokens (ARTs). If the proposal is adopted, crypto-assets other than EMTs/ARTs[1] will benefit from a 'light' regime, subject to simple notification of the relevant NCA rather than *ex-ante* approval. Under this regime, exemptions for small offers[2], offers made only to qualified investors, unique and non-fungible crypto-assets, and crypto-assets merely for use as support for a DLT platform would bring a lighter regulatory touch. A grandfathering clause would be included, exempting any existing crypto-assets in this category from having to comply with title II provisions[3]. Common to all these categories is the requirement of a crypto-asset white paper, detailing the business and technical details of the proposed crypto-currency. Regardless of supervision[4], any issuer would be liable for any losses resulting from impropriety in these white papers, and held to honest, fair and professional standards so as to ensure consumer protection.

E-money tokens

"Electronic money tokens" are a tokenised version of e-money, which are intended to be used primarily as a means of payment. In practice, these would be subject to the same regulatory requirements of EMD2[5], while slightly expanding the definition as to avoid regulatory arbitrage. In order to issue an EMT, authorisation as a credit institution or electronic money institution will be a prerequisite. Issuance and redemption will be required at par value, along with stringent rules in terms of consumer protection, civil liability and asset segregation. The offering of interest on any EMT will be prohibited as well, according to current rules. EMTs can only be issued or offered to the public within the EU subject to these rules. Any EMT denominated in euro or another official currency of the European Union[6] will automatically be assumed to be offered within the EU.

Asset-referenced tokens

Asset-referenced tokens are defined in the draft Regulation as a type of crypto-asset that purports to maintain a stable value by referring to the value of several fiat currencies that are legal tender, one or several commodities or one or several crypto-assets, or any combination these assets. Compared to EMTs, ARTs are to be authorised through a stricter procedure, as outlined in Article 15 *et al.* of the proposal[7]. Of major importance is the legal opinion that these assets do not qualify as financial instruments or other regulated activities. Considering the

1 This is a catch-all definition, including any crypto-asset except for those designated as ART or EMT.

2 Fewer than 150 investors or € 1 million.

3 This primarily entails crypto-asset white paper and marketing communications requirements.

4 NCAs will perform any notification, authorisation and supervisory duties, except where specifically stated otherwise.

5 Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC (Electronic Money Directive or EMD2).

6 Including the Bulgarian lev, Croatian kuna, Czech koruna, Danish krone, Hungarian forint, Polish złoty, Romanian leu, Swedish krona, Swiss franc (in parts of Italy and Germany), and Turkish lira (Cyprus).

7 Including an extensive white paper, containing a description of the issuer's governance arrangements, the reserve of assets, the custody arrangements, the investment policy of the reserve and the rights granted to the holders.

sheer scope of possibilities covered under the ART definition, the challenge lies in regulating activities that have yet to materialise. In response to this, NCAs can refuse authorisation to any issuer where there is a serious risk to financial stability, monetary policy transmission or monetary sovereignty.

Significant EMTs & ARTs

A separate supervisory regime is foreseen for those EMTs and ARTs that are considered to be significant. Classification of one of these crypto-assets is possible at the time of application or upon reaching the thresholds set out in the relevant articles, or at the request of either the issuer or the EBA.

The criteria that will be considered under the MiCA Regulation are the following[1]:

- size of customer base of the asset-referenced token promoters;
- value of asset-referenced tokens/market capitalisation;
- size of the reserve of assets;
- significance of cross-border activity including use for cross-border payments/remittances;
- interconnectedness with financial system.

Additional rules are applicable for any ART or EMT classified as significant, such as higher own funds requirements. Specific rules for ARTs include further interoperability requirements, as well as more thorough liquidity management policies in order to withstand liquidity stress scenarios and renumeration policies that reduce any incentive to relax risk standards. Supervision would be carried out by the EBA in collaboration with a college of supervisors. Significant EMTs, on the other hand, will be subject to addition requirements regarding custody and investment of reserve assets, as well as an orderly wind-down plan. They will have a dual supervisory regime performed by both NCAs and the EBA, also collaborating with the college of supervisors.

Service providers

Acting as a gateway to the financial system, crypto-asset service providers are considered essential in implementing existing regulations in the crypto-sphere. Compliance with rules regarding issuance and offerings to the public are effectively prerequisites for admittance to trading platforms or exchanges.

Typical examples of this category include trading venues, execution and placement, reception and transmission of orders, and advisory services. Drawing upon experience with similar (regulated) services, various rules will be imposed with regard to transparency, consumer protection, conflicts of interest, asset segregation and liability.

Timing

According to the Digital Finance Strategy, the European Commission is hoping that MiCA will enter fully into force by 2024. Allowing for a period of 18 months after entry into force, to complete the necessary RTS, the full proposal would need to be finalised by June 2022.

1 As presented by the EU Commission on 20 September 2020.

Analysing a digital euro – A status update

Filip Caron

An important increase in the pace of change as well as strong potential for disruption are being observed in the retail payments market. Fintech, Bigtech and incumbents have focused on streamlining retail payment – initiation and processing – processes and on improving user experience.

Central banks have the responsibility of fostering efficiency and safety of retail payments in their jurisdiction. In addition to providing a safe and liquid settlement asset by issuing banknotes, central banks play three distinct roles in the retail payments market: operating wholesale payment systems that support transactions between payment service providers in the retail payments market; acting as a catalyst or facilitator of innovation, efficiency and safety in the payments market; and overseeing the resilience, safety and integrity of payment systems.

Recent innovations in retail payments and the continued digitalisation of the economy may weaken central banks' ability to effectively achieve their objectives related to payments, monetary policy and financial stability. Widespread adoption of stablecoins in a foreign currency could impact the effective transmission of monetary policy. Declining use of cash may reduce private individuals' access to a safe and liquid settlement asset. Absence of governing entities in certain crypto-asset arrangements reduces the effectiveness of moral suasion in further enhancing cyber resilience.

Central banks have started to investigate the effectiveness of a central bank digital currency (CBDC) as a response to the challenges they experience in meeting their objectives. More specifically, they are looking into a general purpose CBDC, commonly defined as a digital payment instrument denominated in the national unit of account and a direct liability of the central bank.

The Eurosystem central banks recently published a report outlining key principles and requirements for a digital euro, i.e. a general purpose CBDC (European Central Bank, 2020). According to that report, a digital euro should not compromise economic or financial stability; a digital euro should coexist with cash and non-central-bank money; and a digital euro should promote innovation and efficiency in the retail payments market.

The first section of this article highlights the future scenarios for the retail payments market in which a digital euro could be a viable option to achieve the central banks objectives. Sections 2 and 3 identify key design decisions for a digital euro and its supporting infrastructure, followed by a discussion of the related trade-offs in section 4. The final section discusses the next steps in the continued analysis of the issuance of a digital euro.

A digital euro as a viable option to meet central bank objectives

Continued digitalisation of retail payments has been observed and has even accelerated during the COVID-19 pandemic (e.g. the portion of contactless payments – compared to all retail payments in Belgium – more than doubled over the course of 2020 (Febelfin, 2021)). Moreover, as retail payments solutions are subject to network economics, where a solution becomes more useful as the number of users increases, a recent push for further globalisation under the impetus of Bigtech firms has been observed (e.g. the Libra/Diem project supported by Facebook). Both digitalisation and globalisation could have an impact on achievement of central bank objectives.

The Eurosystem has identified a series of realistic future scenarios for the retail payments market, in which a digital euro could be a viable option to meet central bank objectives. These possible scenarios have not materialised yet and should not be considered as mutually exclusive.

Supporting further digitalisation of the economy by meeting emerging payment needs

General purpose CBDCs filling gaps in the current provisioning of digital payment services could facilitate further digitalisation of the financial sector and the broader economy. For example, a digital euro could foster inexpensive pan-European digital payment services that are not subject to data analysis. So, a digital euro could become an important building block for an integrated, secure and efficient pan-European retail payment infrastructure.

Despite all efforts to further integrate the retail payments market in Europe, the European Central Bank has noted limited cross-border acceptance for domestic card schemes (European Central Bank, 2019). Ten European countries' national card schemes still do not accept cards from other EU Member States. Foreign payment solutions have benefited from this gap in the European payment ecosystem and have taken the lead here. Most cross-border payments within Europe go through two international card schemes: Visa and MasterCard.

Widely adopting foreign payment solutions should not be an issue if the same business, same risk, same regulation principles are followed, and if there is appropriate oversight. However, the changing geopolitical context has been marked by an increase in protectionist policies. Geopolitical sanction regimes or even exclusions from payment systems could result in significant risks of payment disruptions in certain jurisdictions.

A digital euro could support the recent pan-European retail payment strategy. This strategy centres on five key objectives: "full pan-European reach and unified customer experience; convenience and cost efficiency; safety and security; European identity and governance; and, in the long run, global acceptance". By design, a digital euro would be a pan-European solution with appropriate attention for efficiency and safety. Furthermore, research by the Bank for International Settlements has confirmed that a general purpose CBDC could foster competition (Bank for International Settlements, 2020).

The objective should not be to crowd out private solutions. Both a digital euro and the European Payments Initiative (EPI) could form an integral part of this strategy. A public-private partnership for distributing and supporting payments in central bank money would validate the intermediated model which is preferred by the Eurosystem.

Other gaps in the provision of payment solutions and functionalities may occur, including the lack of programmability and support of micropayments. For instance, the digital euro report examines the possibility of including conditional payments. Micropayments or small low-cost payments will be needed to support the development of the Internet of Things.

Providing a digital form of public money in response to a significant decline in the use of cash

If the use of cash is marginalised, greater dependence on private forms of money and their supporting infrastructure would be observed. The Eurosystem may decide to issue a digital euro to continue guaranteeing access to a form of public money, characterised as a widely accessible, cheap and safe payment instrument. Bearer instruments for a digital euro would continue to support financial inclusion across the euro area in an increasingly digitalised payments market. Furthermore, the Eurosystem central banks will never analyse payment data for upselling or marketing purposes.

The European Central Bank's 2020 Study on the payment attitudes of consumers in the euro area (SPACE) confirmed that consumers predominantly use cash as a payment instrument for person-to-person and business-to-customer transactions (European Central Bank, 2020). The latter includes both payments for online purchases and purchases at physical points of sale. In 2019, 58 % of retail payments in Belgium were carried out using cash as the payment instrument. With the reported 73 % of retail payments volume conducted using cash, the stakes are even higher for the euro area.

However, the self-reported preferences for payment instruments in the SPACE report indicate that about half of the respondents prefer cards or other cashless payment instruments. Another quarter is indifferent between cash or a cashless payment instrument. This may highlight a mismatch between the end user's preference and the accepted payment instrument in various situations.

Furthermore, there are countries in the euro area that have been observing a significant decline in the use of cash, e.g. only a third of retail payments in the Netherlands were made in cash.

Tackling monetary sovereignty issues when non-euro denominated money becomes omnipresent in the euro area

Widespread adoption of alternative digital currencies, e.g. a foreign CBDC or private non-euro denominated stablecoins, could severely affect the status of the euro as a unit of account. This could have implications for monetary policy, financial stability and the safety and efficiency of European payments. An efficient and convenient digital euro could reduce the risk of currency substitution.

Maintaining price stability is the primary objective of monetary policy. To this end, the ECB Governing Council sets the interest rates at which financial institutions borrow euros from and deposit euros at the central bank [1], which in turn affects borrowing conditions in the economy. The effectiveness of the monetary policy transmission of a central bank is largely based on the strong dominance of the currency it issues.

Secondly, the ability of the central banks in the euro area to act as lender of last resort could be significantly weakened, if financial institutions start to accept substantial deposits in alternative currencies. Central banks cannot provide unlimited quantities of alternative digital currencies to solvent banks during liquidity crises.

Thirdly, increasingly dominant alternative digital currencies could pose major challenges for the Eurosystem in maintaining the efficiency and safety of payment systems. Alternative digital currencies offered by entities outside the supervisory scope of the European authorities could be made available to European citizens. There are no guarantees that these entities are following the same strict safety and efficiency standards as those overseen and supervised by the European authorities.

Fourthly, the financial intermediation strategies and the incentives of entities issuing alternative currencies remains unclear. There are no guarantees that financial institutions in the euro area could play any significant

1 Since the financial crisis, non-standard measures have been taken as well.

intermediation role, which could mean significant risks for financial stability. But incentives for the issuers of alternative currencies could pose important risks, too. For example, these issues may decide to create money in excess of the money demand to generate additional seigniorage for its shareholders, which may result in a heightened inflation.

Currently, the currency substitution scenario is not materialising but there are important risks related to the speed at which it may materialise. BigTech firms could leverage strong international user bases to gain a substantial market share for an alternative digital currency. Additional competitive advantages stem from their extensive experience in designing integrated and user-friendly solutions. Furthermore, extensive reward schemes offered by BigTech firms could be an effective tool in stimulating the adoption of alternative digital currencies.

Reinforcing monetary policy transmission

An interest-bearing and universally accessible digital euro could further improve the effectiveness of the monetary policy. The ECB's Governing Council could adapt the remuneration of a digital euro to influence the level of investment and consumption in the euro area. Reducing remuneration during economic crises could boost aggregate investment and consumption.

The remuneration offered by a digital euro will act as a floor for deposit rates offered by commercial banks. Researchers have suggested that offering depositors an outside option will be enough to influence the deposit market and make it more competitive, even if the CBDC is not widely accepted (Davoodalhosseini *et al.*, 2020).

In contrast to cash, a digital euro could be negatively remunerated. Removing this effective lower bound would require important restrictions on the usage of cash, to avoid a move into cash to escape from negative interests. Examples of these restrictions include limiting cash withdrawals and deposits; removing large-denomination notes; or even eliminating cash. A negatively remunerated digital euro explicitly violates the principles set out by the Eurosystem and is therefore not considered in the current analyses (European Central Bank, 2020).

Additionally, a digital euro could theoretically be used for the distribution of helicopter money. Fair distribution of helicopter money would require access for all citizens, as well as the ability to uniquely identify individual citizens in the underlying infrastructure (to avoid "double spending" by the government).

Preparing for extreme events

Cyber incidents, natural disasters and other extreme events form an integral part of the threat landscape in which financial institutions and retail payments operate. Prolonged outages of payment solutions like card payment schemes and mobile payment applications could affect European retail payments and erode trust in the overall financial system.

The European Systemic Risk Board recently identified cyber threats as a source of systemic risk for the financial systems, deeming that it could have severe negative consequences for the European economy (European Systemic Risk Board, 2020). Furthermore, different service providers appear to be increasingly dependent on a small set of technologies and service providers (e.g. cloud providers). As a result, a major incident related to these technologies and/or service providers could have a significant impact across various retail payment solutions.

Currently, cash acts as an effective back-up system during extreme events, i.e. cash immediately guarantees the transfer of funds in exchange for delivered goods or services. This would no longer be possible in a future scenario characterised by much lower or even marginalised cash use.

A widely adopted digital euro could act as a back-up system, under strict conditions. Firstly, the underlying payment infrastructure should be independent from current solutions and developed with technology diversity in mind (i.e. based on different technology wherever possible). Secondly, the underlying payment infrastructure should comply with the strictest security and resilience requirements.

Designing an attractive payment instrument

The instrument design analysis should formulate an opinion on three fundamental questions. Should a digital euro be remunerated? Should access to and/or holdings in digital euro be restricted? Should digital euro holdings and transactions be private?

Renumeration and incentive design

The inability to pay or receive interest on physical cash is an important technological constraint, which could be overcome with a digital euro.

If a digital euro were remunerated, a series of additional incentive design decisions would need to be considered. Firstly, the interest rate could be positive but (theoretically) a negative interest rate could be set, too. A negative interest rate would require political acceptance.

Secondly, the incentive design could include various types of interest differentiation. A tiering of the interest rate has been presented in multiple publications (Bindseil & Panetta, 2020). This implies that the remuneration of the digital euro is relatively attractive up to a quantitative ceiling, while significantly lower interest rates are applied for holdings above the interest rate. But interest differentiation could also be implemented based on stakeholder type. For example, for corporates or foreigners, the quantitative ceiling could be set to zero or calculated based on presumed payments needs (Bindseil, 2020).

Finally, the conceptual design will need to consider whether the interest rate should be fixed or allowed to fluctuate over time.

Restrictions on access to and holdings in a digital euro

The instrument design may define limits on the amount of digital euro that each individual, household or business could hold. These restrictions on access could reinforce a role as payment instrument.

Implementing maximum holding limits should be technically straightforward for centralised infrastructures, which are based on currently dominant architectures. Payees would not be able to accept payments that would result in their current balance exceeding the maximum holding. This solution could be considered sub-optimal as it would implicitly expose sensitive information on the current balance of the payee. Moreover, it would create additional friction as payments could be automatically rejected. Alternatively, the amount in excess of the maximum holding limit could be directly transferred to an account held by the payee with an authorised financial institution (Panetta, 2018). This second solution would require each user of a digital euro to open an account with a financial institution in the euro area.

The feasibility of implementing maximum holding limits in a DLT-based back-end infrastructure has been demonstrated in a proof-of-concept developed by European System of Central Banks' EUROchain research network (European Central Bank, 2019). If the maximum holding limit of the payee were exceeded by accepting the payment, the payment would be automatically rejected.

Furthermore, access and holding restrictions for individuals and businesses outside the euro area will need to be reviewed. Only a limited number of these stakeholders are expected to have access to an account with a financial institution in the euro area.

Degree of privacy offered by a digital euro

Different privacy constructs could be considered when designing a digital euro. The conceptual analysis should consider which types of information need to be kept private under which conditions and from whom to keep it secret. There is no binary choice between full anonymity and full disclosure.

Information regarding digital euro holdings and transactions could be shielded from a variety of stakeholders, including transaction counterparties, payment service providers, governments and the general public. A recent article pointed to a series of interesting techniques that could be adopted in the design (Darbha & Arora, 2020). Zero-knowledge proofs can be used to prove claims about data without disclosing any actual data, which could be used to prove that a payer has sufficient funds. Homomorphic encryption could be used to calculate the remuneration that needs to be paid while the balance remains encrypted. Multi-signature approaches could allow for decryption of sensitive data if an appropriate number of entities agree to its disclosure.

A recent proof-of-concept developed by the European System of Central Banks demonstrated that it is technically feasible to offer different levels of privacy depending on the value of the transaction (European Central Bank, 2019). This would allow for high degrees of privacy for lower-value transactions, whereas large-value transactions would be subject to AML/CFT[1] checks by a dedicated authority.

Designing a system to support the digital euro

The Eurosystem will examine all the different options to support payments in a digital euro. At the core of the settlement process lies a ledger to record the underlying transfers of central bank liabilities. Different alternatives to initiate payments in digital euro could be considered, as well as the potential role of financial intermediaries.

Back-end infrastructure

A broad variety of ledger design and structure options have emerged lately. The back-end infrastructure could be based on a centralised or decentralised architecture, as well as account-based or value-based. Additionally, the ledger could potentially be further enriched with smart contract functionality, resulting in programmable money. Infrastructure design choices should be grounded in user requirements, and not be dictated by technology choices.

Decentralised and distributed ledgers have been adopted by a vast series of cryptocurrencies. Research has identified potential opportunities for enhancing both the efficiency and safety of this technology for payment systems (Committeee on Payments and Market Infrastructures, 2017). Furthermore, a decentralised infrastructure could more easily facilitate offline peer-to-peer transactions. The design must ensure that digital euro holdings and transactions are recorded in line with the rules set by the central bank.

But centralised ledgers with the central bank as intermediary to record all transactions, should not be excluded without proper analysis. Centralised ledgers may facilitate an easier implementation of fraud and compliance detection (Bank for International Settlements, 2020). With the TARGET instant payment settlement (TIPS)

1 Anti-money-laundering / Combating the financing of terrorism.

system, the Eurosystem has already established the core components of such an architecture (European Central Bank, 2020).

Two alternative authentication approaches are commonly discussed: value-based and account-based authentication. A value-based digital euro would centre on the users' ability to verify that the digital object is genuine, typically through encryption keys. This approach could enable offline payments.

Account-based authentication relies on a third party – like the central bank or an accredited third-party – to verify the users' identity to confirm the validity of a transaction. Account-based authentication is compatible with both centralised and decentralised ledgers, examples include respectively TIPS and Ethereum. While scaling-up the number of accounts may sound straightforward and not necessarily innovative, multiple researchers have suggested that significant technical challenges would need to be addressed (Bindseil, 2020).

Finally, programmable money has been garnering a great deal of attention. In addition to simple record-keeping, the back-end infrastructure could verify whether payment conditions have been met. End users could specify timing and sequencing conditions for payments. Other applications could include the earmarking of specific balances – e.g. for healthcare or food expenses – which result in the creation of non-fungible money.

Access via intermediaries

Central banks could opt to provide the public with direct access to a general-purpose CBDC or with access through supervised intermediaries. The former may imply that the central banks conduct a series of end-user-facing services, like customer identification, compliance checks and end-user support. This would imply a significant expansion of the scope of central banks' activities.

The Eurosystem expressed a clear preference for the intermediated model (European Central Bank, 2020). Two distinct roles could be attributed to supervised intermediaries, i.e. intermediaries could be mere gatekeeper or full settlement agents. Intermediaries acting as a gatekeeper would focus on authenticating end users and conducting the end-user-facing activities. These are activities similar to those conducted by commercial banks in the distribution of cash.

Supervised intermediaries could also act as settlement agents. End users provide payment instructions to the supervised intermediary of their choice, e.g. a commercial bank. These settlement agents instruct or execute the transfer of digital euro units on behalf of their customers. As the central bank would only interact with supervised intermediaries, the number of connections to the system would be significantly lower.

Appropriate supervision should ensure that the activities of these intermediaries do not affect trust in a digital euro and that appropriate measures to preserve the central bank liability nature are implemented. This includes measures that prevent the creation of additional digital euro units as a result of errors or misconduct.

Access solutions

Access solutions link stakeholders with the back-end infrastructure. Stakeholders include private individuals holding digital euro, merchants accepting payments in digital euro and all supervised intermediaries. Access solutions should support authentication and authorisation requirements, enable universal access and guarantee interoperability with other services in the European financial ecosystem.

A broad variety of software-based payments solutions have been widely adopted in the euro area, including mobile banking apps and web browser-based online banking. These solutions support various use cases, ranging from peer-to-peer transactions to payments in the context of e-commerce. The underlying concepts are valid for gaining access to digital euro holdings or initiating payments in digital euro.

Hardware-based payment solutions or payment devices serve multiple purposes, including financial inclusion and offline transactions. Offering payment devices to private individuals potentially without a smartphone will increase financial inclusion and support the universal access objective. Dedicated devices could theoretically also support offline device-to-device payments, which may also reinforce resilience under extreme circumstances. In a recent publication, the Bank for International Settlements suggests active engagement with cognitively- or sensory-impaired users to further enhance financial inclusion (Bank for International Settlements, 2020).

Additional application programming interfaces (APIs) could enable supervised intermediaries to integrate the digital euro in their service offering. Furthermore, design choices on the interoperability with non-euro payment systems could have a significant impact on a digital euro's global reach. Due attention needs to be paid to compatibility solutions, as well as links with other CBDC systems that may emerge.

Interplay between design choices and central bank objectives

Decisions regarding the design of the digital euro are not discrete and interdependent. Agreeing on a coherent set of design decisions will be essential to the development of an effective and efficient digital euro.

Additionally, design decisions will impact the efficiency of the digital euro as a tool to achieve central bank objectives. Design decisions typically impact multiple central bank objectives; and could be supportive of one objective while at the same time negatively impacting another.

Privacy is a top priority for prospective users of a digital euro, as was highlighted in a recent consultation organised by the Eurosystem. However, an interesting trade-off between privacy and the desire to reduce the scope for criminal activity has been identified. This trade-off should not be considered the sole responsibility of the central banks, but part of a broader discussion in the European community.

This section will further elaborate on the interplay between design choices and central bank objectives and highlight important interactions between the central bank objectives (limited to those important in the context of a CBDC).

Effects on financial institutions and safeguarding financial stability

Issuing an efficient digital euro will almost inevitably result in a partial substitution of cash and commercial bank deposits for that digital euro. A substitution of commercial bank deposits for digital euro holdings will lead to a reduction in funding for banks, which, if not appropriately covered, may imply disintermediation.

Commercial banks may seek to reduce the level of disintermediation through bundling of services (including mortgage and other loans) or more attractive remuneration than the digital euro. The latter could have an important impact on the commercial banks' cost of funding. Alternatively, commercial banks could replace lost deposit funding with longer-term deposits or central bank funding. But these alternatives could also raise the overall cost of funding.

If commercial banks do not want to erode their franchise value, they could revise the terms of the loans which they provide to the economy. An increase in the cost of borrowing may result in a lower volume of lending and impact economic activity, all else being equal. Or commercial banks could decide to take on greater risks to safeguard their profitability.

Multiple researchers have suggested that a CBDC could further facilitate a run on the banking system. Especially if a digital euro were easily (and unrestrictedly) convertible into other forms of euro denominated money.

During financial crises, a risk-free asset like the digital euro could be considered immensely more attractive by households and businesses.

The design of a digital euro may highly influence the extent of the disintermediation effect. Remuneration will likely be an important driver of the attractiveness of a digital euro. To minimise disintermediation, the central bank may opt not to remunerate or offer a rather unattractive rate compared to that offered by the commercial banks.

Adopting tiered remuneration could allow for an attractive payment instrument while removing the incentive to use a digital euro as a store of value. This would require attractive remuneration up to a quantitative ceiling (tier one), while above that threshold, an unattractive remuneration would be applied (tier two). It could be decided to cap digital euro holdings to the quantitative ceiling altogether.

Effects on monetary policy

An attractively remunerated digital euro with wide access – not limited to financial institutions – could support the implementation and transmission of monetary policy to the real economy. If the digital euro design allows for negative remuneration, it could help alleviate the effective lower bound, particularly if combined with reduced supply of non-remunerated cash. This is discussed in the monetary policy future scenario, but would violate the requirements specified by the Eurosystem. Digital euro designs in which access and/or holding restrictions are adopted reduce the scope for a more direct pass-through of the policy interest rates.

Remuneration is a design factor that will determine the impact on both the financial stability and monetary policy, as a digital euro could compete with bank deposits. In the event of large bank runs, central banks could mitigate the impact on commercial banks by reducing (considerably) the rate of remuneration of a digital euro.

Flows into and out of digital euro may have an impact on the central banks' balance sheets. For example, if bank deposits are substituted for digital euro units or unrestricted access for non-residents would be allowed, the central bank's liabilities would increase. As a result, central banks will need to acquire more assets on their balance sheets. The Eurosystem central banks have discretion in selecting the assets that they will hold, e.g. any kind of collateralised lending or asset holdings. But subject to the overall supply of different asset classes (as well as changes thereof) and the volatility in demand of a digital euro, central banks might face additional duration, liquidity and credit risks.

The cost-benefit analysis of using a digital euro as an additional monetary policy tool is not yet clear. Doubts have been raised about the need to strengthen the transmission channels, as well as the effectiveness of a digital euro in attaining monetary policy objectives (Bindseil, 2016). Furthermore, other conventional tools may be as effective in achieving the monetary policy objectives.

Outlook

With its October 2020 report on a digital euro, the Eurosystem defined a set of key principles and requirements for a digital euro. The report formed the basis for a dialogue with all stakeholders on the objectives and potential design options. Initial consultation responses identified privacy as the most requested feature of a potential euro (mentioned in 41 % of the replies), followed by security (17 %) and pan-European reach (10 %).

Between October 2020 and July 2021, the Eurosystem central banks conducted a series of practical experiments to further explore the technical feasibility of the different systems and instrument design options. This is to be

followed by a formal decision of the Governing Council on whether or not to continue investigating a digital euro. No decisions regarding the issuance of a digital euro have been made yet.

The NBB and ECB will continue to proactively interact with the different stakeholders in a digital euro – including prospective end users and supervised intermediaries – to accurately sound out their requirements.

In addition to the technical and functional analyses, the Eurosystem continues to actively examine policy-oriented challenges and the legal aspects of a potential digital euro.

Bibliography

Bank for International Settlements, 2020. BIS Annual Economic Report 2020. [Online] Available at: https://www.bis.org/publ/arpdf/ar2020e3.pdf.

Bank for International Settlements, 2020. Central bank digital currencies: foundational principles and core features. [Online] Available at: https://www.bis.org/publ/othp33.pdf.

Bindseil, U., 2016. Evaluating monetary policy operational frameworks. [Online] Available at: https://www.kansascityfed.org/~/media/files/publicat/sympos/2016/econsymposium-bindseil-paper.pdf?la=en.

Bindseil, U., 2020. Tiered CBDC and the financial system (working paper series No 2351). [Online] Available at: https://www.ecb.europa.eu/pub/pdf/scpwps/ecb.wp2351~c8c18bbd60.en.pdf.

Bindseil, U. & Panetta, F., 2020. Central bank digital currency remuneration in a world with low or negative nominal interest rates. [Online] Available at: https://voxeu.org/article/cbdc-remuneration-world-low-or-negative-nominal-interest-rates.

Committeee on Payments and Market Infrastructures, 2017. Distributed ledger technology in payment, clearing and settlement. [Online] Available at: https://www.bis.org/cpmi/publ/d157.pdf.

Darbha, S. & Arora, R., 2020. Privacy in CBDC technology. [Online] Available at: https://www.bankofcanada.ca/2020/06/staff-analytical-note-2020-9/#:~:text=Bank%20of%20Canada%20research%20has,of%20anonymity%20or%20full%20disclosure.

Davoodalhosseini, M., Rivandeneyra, F. & Zhu, Y., 2020. CBDC and monetary policy. [Online] Available at: https://www.bankofcanada.ca/2020/02/staff-analytical-note-2020-4/.

European Central Bank, 2019. Card payments in Europe – Current landscape and future prospects: a Eurosystem perspective. [Online] Available at: https://www.ecb.europa.eu/pub/pdf/other/ecb.cardpaymentsineu_currentlandscapeandfutureprospects201904~30d4de2fc4.en.pdf.

European Central Bank, 2019. Exploring anonymity in central bank digital currencies. [Online] Available at: https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.mipinfocus191217.en.pdf?3824c3f26ad2f928ceea370393cce785.

European Central Bank, 2020. Report on a digital Euro. [Online] Available at: https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf.

European Central Bank, 2020. Study on the payment attitudes of consumers in the euro area (SPACE). [Online] Available at: https://www.ecb.europa.eu/pub/pdf/other/ecb.spacereport202012~bb2038bbb6.en.pdf.

European Systemic Risk Board, 2020. Systemic cyber risk. [Online] Available at: https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf?fdefe8436b08c6881d492960ffc7f3a9.

Febelfin, 2021. Coronamonitor voor januari 2021. [Online] Available at: https://www.febelfin.be/sites/default/files/2021-01/Dashboard-2021-01-28-NL.pdf.

Panetta, F., 2018. 21st century cash: Central banking, technological innovation and digital currencies. [Online] Available at: https://www.suerf.org/policynotes/3251/21st-century-cash-central-banking-technological-innovation-and-digital-currencies.

Digital operational resilience

Thomas Plomteux

Assessing cyber and ICT risks as well as encouraging control over those risks are key priorities for the Bank in the exercise of its different missions. This article takes a look at the cyber and ICT-related threats and risks facing financial institutions in general and market infrastructures, payment institutions and electronic money institutions in particular. This is followed by a summary of the various initiatives taken by the Bank in this context. Finally, there is an overview of common observations made during on-site inspections focused on cyber and ICT risk, also with particular attention to FMIs, PIs and ELMIs.

Continuing rise in cyber and ICT threats

In 2020 and the first half of 2021, the digital operational resilience of the financial sector was tested to a considerable degree by the COVID-19 pandemic. Since March 2020, companies and institutions have largely switched to working from home, which poses unprecedented challenges and additional risks. Initially, these challenges were mainly operational, such as the need to expand IT capacity for teleworking. As the pandemic drags on, the challenges are becoming increasingly strategic in nature. For instance, institutions are being forced to set priorities between current and planned strategic projects, the current circumstances often preventing them from maintaining their pre-crisis pace and extent of change. Furthermore, while wide-scale teleworking reduces the health risk, it heightens the inherent cyber and ICT risks. Some institutions may have had to temporarily adjust their security controls in order to facilitate this remote working. Additionally, the reduced physical availability of operators can make it more difficult to resolve incidents, or the large number of company computers simultaneously connecting remotely to the institution over the internet can present challenges. Fortunately, owing to the precautions taken by the institutions, this situation has not yet led to any major operational incidents.

In any case, cyber attacks have become an everyday reality throughout the world in recent years. Attackers are also evidently refining the techniques and methods used, so that some of the attacks are becoming ever more sophisticated and powerful. The number of persistent, targeted cyber attacks is therefore likely to increase further in the future, with the financial sector logically remaining a potential target. The list of cyber attacks targeting financial institutions worldwide drawn up by the think tank Carnegie Endowment for International Peace[1] provides an up-to-date view of the cyber threats facing the sector. An additional example is the large-scale attack on SolarWinds, a global service provider of software for network, system and infrastructure management. The impact of this attack on SolarWinds customers is still being mapped today.

1 https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline.

In these circumstances, it is challenging for financial institutions and infrastructures to provide adequate protection for their IT systems, services and data against all the various attacks. As cyber threats are evolving very rapidly, it is more necessary than ever to ensure that the defence capability of financial institutions and FMIs enables them to respond flexibly to changing patterns of attack. It is vital in this regard to have solutions for collecting data on potential threats, attackers and types of attack. It is also important not only for the external perimeter of the institution's network to be properly secured and monitored, but also for the internal measures to be sufficiently fine-meshed, incorporating multiple layers of protection. For financial institutions, it is likewise useful to know the risk profile of the customer and/or counterparty when determining the risk of fraud for certain transactions. In the context of retail banking, for example, that involves the use of security mechanisms built into the mobile or online banking application. As regards correspondent banking activities, examples include the Customer Security Programme (CSP) developed by SWIFT to assist financial institutions in assessing the counterparty risk relating to their messaging traffic. The CSP also stresses the importance of frequent reconciliation of outgoing transactions, to ensure prompt detection of potentially fraudulent activities and, where necessary, to stop them before they reach their final destination.

Apart from cyber risks, the financial sector's heavy dependence on IT solutions also presents other challenges. Under pressure from innovative players and customer expectations regarding the services offered, traditional institutions are being forced to renew their sometimes outdated IT architecture in a relatively short period of time. Growing security risks, e.g. from the use of end-of-life software that is no longer supported, may also lead to such a need. However, in some cases, the complexity of these institutions' IT environment makes it a major challenge to achieve this in a responsible way. There is likewise a high risk of growing dependence on third parties for IT services and other standardised IT system components. In particular, cloud solutions are increasingly being used, and for ever more important processes. That is also among the reasons why, throughout the sector, a small number of critical service providers present an ever-increasing concentration risk for the financial industry. The need for sufficiently representative testing of developed software and recovery solutions for various extreme but plausible scenarios remains another key point of focus.

It is therefore important for financial institutions' management bodies to have the necessary expertise and information to monitor risks appropriately, and to incorporate adequate measures in their strategic planning in order to keep risks within acceptable limits. However, many institutions say they have difficulty in recruiting sufficient staff with the required skills and expertise. In addition, all the staff of those institutions must be aware of the cyber and ICT risks in order to understand how those risks can arise and be ready to respond to them as expected.

Regulatory and operational initiatives

In recent years, the Bank has made a substantial contribution to the development of a regulatory framework aimed at improving the control of cyber and ICT risks. The prudential Circular on the Bank's expectations regarding operational business continuity and security of systemically important institutions[1] remains a key reference point. The Bank is also making an active contribution to establishing a European regulatory framework for the management of cyber and ICT risks. Under the aegis of the EBA, this has led to the publication of guidelines for supervisory authorities on the assessment of the ICT risk in the SREP[2], guidelines on outsourcing[3], and guidelines on ICT and security risk management[4]. These guidelines have since all become part of the Bank's supervision and policy framework.

1 Circular NBB_2015_32 of 18 December 2015 on the additional prudential expectations regarding operational business continuity and security of systemically important financial institutions.

2 EBA Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation Process (SREP) (May 2017).

3 EBA Guidelines on outsourcing arrangements (February 2019).

4 EBA Guidelines on ICT and security risk management (November 2019).

In September 2020, the European Commission published a proposal for a Regulation called the Digital Operational Resilience Act (DORA). The Bank also plays an important advisory role in the Belgian delegation for discussions on draft legislation at European level, and will probably also be closely involved in complementing DORA with technical standards. More information on this subject can be found in box 13.

The approach concerning individual institutions is two-pronged. On the one hand, institutions subject to prudential supervision are required to hold capital to cover their operational risks, including cyber and ICT risks. At the same time, the operational security and robustness of the critical processes of financial institutions and FMIs are subject to close monitoring. The availability, integrity and confidentiality of IT systems and data are crucial here. In 2020, the Bank once again conducted a number of inspections to check on compliance with the regulatory framework and to verify proper management of IT systems in relation to cyber and ICT risks. In addition, the Bank monitors these risks in financial institutions and FMIs in the course of its ongoing and recurrent supervisory activities. The COVID-19 health crisis forced the Bank to review its approach to these supervisory activities. The content of the activities was adjusted to the new reality, with particular emphasis on COVID-19, while working methods were adapted to give preference where possible to remote meetings and technological resources. Finally, the Bank operationalised a framework for ethical hacking, which is discussed in the thematic article on Threat Intelligence-Based Ethical Red teaming in Belgium (TIBER-BE).

The Bank is also paying closer attention to sectoral initiatives. Prompted by the SSM, among other things, some FMIs are regularly asked to complete an IT questionnaire which provides important data for the annual SREP and also permits cross-sectoral analyses. In its role as the sectoral authority for application of the Law on the security and protection of critical infrastructures (principally systemically important banks and FMIs), the Bank also assesses the effectiveness of the control systems of critical financial infrastructures. In that context, the Bank organises and coordinates sectoral crisis simulation exercises in order to prepare the Belgian financial sector for potential operational incidents of a systemic nature, should they occur in the future. Under the Law on network and information system security (NIS), the Bank acts as the sectoral point of contact for major incidents in the financial sector.

BOX 13

Digital Operational Resilience Act

Context

On 24 September 2020, the European Commission's Directorate-General for Financial Stability, Financial Services and Capital Markets Union (DG FISMA) presented its proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector, the so-called Digital Operational Resilience Act (DORA)[1]. This piece of legislation is part of a much broader Digital Financial Strategy that sets out general lines on how Europe can support the digital transformation of finance in the coming years, while regulating and mitigating the risks arising from it.

The proposal for a Regulation on digital operational resilience is motivated by the ever-increasing dependence of the financial sector on software and digital processes, resulting in information and

1 COM/2020/595 final – https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12090-Digital-Operational-Resilience-of-Financial-Services-DORFS-Act.

communication technology (ICT) risks posing a challenge to the operational resilience, performance and stability of the EU financial system as a whole. The Commission tabled the proposal because it believes that current legislation across Member States does not fully address the topic, nor does it provide financial supervisors with the most adequate tools to fulfil their mandates, and leaves too much room for diverging approaches across the Single Market. Last but not least, the proposal responds to the 2019 Joint Technical Advice of the European Supervisory Authorities (ESAs) that called for a more coherent approach in addressing ICT risk in finance[1].

The DORA proposal contains five distinct pillars:

- **Governance-** and **ICT-risk-management-**related key principles and requirements for financial entities, inspired by relevant international, national and industry-set standards, guidelines and recommendations. These requirements revolve around specific functions in ICT risk management (identification, protection & prevention, detection, response & recovery, learning & evolving, and communication), but also underline the importance of an adequate governance and organisational framework. Amongst others, the crucial, active role the management body has in steering the ICT risk management framework and the assignment of clear roles and responsibilities for ICT-related functions is covered by this first pillar.
- The second pillar relates to requirements for financial entities with regard to **managing** and **classifying ICT-related incidents**, and a proposal to harmonise and streamline the **reporting** of such major incidents to the competent authorities, alongside responsibilities for competent authorities in providing feedback and guidance to financial entities and in forwarding relevant details to other authorities with a legitimate interest. The ambition put forward is that financial entities should report major incidents only to one competent authority. To this end, the feasibility of a single EU hub will be studied by the ESAs, the ECB and ENISA.
- The third pillar addresses requirements for **digital operational resilience testing**, i.e. periodically testing for preparedness and identification of weaknesses, deficiencies or gaps, as well as the prompt implementation of corrective measures. While all financial entities should test their ICT systems by making use of tests ranging from vulnerability scanning to software code analysis, only those entities identified by competent authorities as significant and cyber mature will be required to conduct advanced Threat-Led Penetration Tests.
- Fourth, there are provisions that should ensure the sound management of **ICT third-party risk**. On the one hand, this objective will be achieved through the respect of **principle-based rules** applying to financial entities' monitoring of this risk, and through regulation **harmonising key elements** of the service and relationship with ICT third-party providers. On the other hand, the regulation seeks to promote convergence on supervisory approaches to ICT-third-party risk in the financial sector by **subjecting critical ICT third-party service providers to an EU oversight framework**.
- Fifth, to raise awareness on ICT risk, to minimise the propagation of risk, to support financial entities' defensive capabilities and threat detection techniques, the regulation explicitly allows financial entities to set up arrangements to **exchange** amongst themselves **cyber threat information and intelligence**.

The foreseen scope of application of DORA is a broad range of financial entity types, amongst others credit institutions, insurance and reinsurance undertakings, investment firms, payment institutions and

1 Joint Advice of the European Supervisory Authorities to the European Commission on the need for legislative improvements relating to ICT risk management requirements in the EU financial sector, JC 2019 26 (2019).

electronic money institutions. By having this broad scope, DORA seeks to harmonise approaches across the financial sector with the objective of an increased operational resilience and to ensure a safer overall financial system. A lighter regime is on the cards for microenterprises[1].

Points of focus for the National Bank of Belgium

Since the publication of the DORA proposal, experts from the National Bank have contributed to defining the Belgian position that is reflected in discussions on this proposal in the EU Council's Working Party on Financial Services, held first under the German and now the Portuguese presidency. It is to be expected that the NBB experts will also play a role in the development of the regulatory and implementation technical standards that will support the final DORA Regulation.

Overall, the NBB is very supportive of the DORA initiative and its ambition to strengthen digital operational resilience and to further harmonise ICT risk management practices and requirements in the financial sector. In some areas, there are nevertheless some issues that warrant further discussions in the Working Party so as to clarify the exact scope and impact of the Regulation. Some examples are the following:

- *Proportionality principle* – In order to avoid imposing undue burdens on smaller financial entities and smaller ICT third-party providers, the DORA proposal should be scrutinised to include some further exemptions from its provisions; and/or some DORA provisions could be modulated according to the size and/or criticality of the financial entities in scope.
- *Scope of DORA* – The rationale for including external auditors and insurance intermediaries in the scope of application of the Regulation needs to be further investigated and clarified. On the other hand, the exclusion of payment systems, card schemes and clearing and settlement systems from the scope is welcomed, since these are typically already covered by the oversight of central banks, with a well-developed and harmonised framework set up by national central banks and the ECB.
- Another element of scope that warrants further clarification is the current definition of "ICT services" and "ICT third-party providers". As both terms are defined in a very wide sense, this could lead to the unintended inclusion of several service providers that are better left out of the scope of DORA. In particular, undertakings whose core business is in the processing of payment transactions come to mind. In Belgium, such processors of payment transactions are already subject to a specific oversight regime.
- *Concurrent legislative undertakings* – While the text of the DORA Regulation is being negotiated, discussions on a revised NIS directive on the Security of Network and Information Systems (NIS 2) have also started. To avoid overlap and collusion between both undertakings, the relationship between them should be clarified and clearly delineated. While DORA is a Regulation specific to the financial sector, the renewed NIS Directive could be transposed differently across EU countries and is not limited to the financial sector but has a more transversal scope across industries.
- *Interplay between PSD2 and DORA* – With regard to major incident reporting, the interplay between the PSD2 Directive and DORA needs to be clarified. More specifically, any doubt should be removed as to the competent authority that should receive the incident reports directly from the reporting entity. With DORA being limited to the reporting of ICT incidents, further clarification should also be provided on the treatment of non-ICT related incidents as foreseen under PSD2.

1 As defined in Commission Recommendation 2003/361/EC, a microenterprise is an enterprise which employs fewer than 10 people and whose annual turnover and/or annual balance sheet total does not exceed € 2 million.

- *Recognition of well-established TIBER-EU framework* – Regarding advanced digital resilience testing, the Eurosystem already developed harmonised Threat Lead Penetration Testing standards and practices with its TIBER-EU framework. So, DORA provisions on advanced digital resilience testing could be largely based on referencing the TIBER-EU framework. Valuable characteristics of the current TIBER-EU approach could thus be maintained (e.g. the planning of tests based on constructive dialogue; mutual recognition principles) and not all competent supervisory authorities should become operationally involved in the tests, nor should they validate the correct execution or the results of the tests. Involving competent authorities when discussing the scope of a test and incorporating test results into their supervision could be beneficial.
- *Provisions on outsourcing* – Concerning ICT third-party management, wording in DORA can be clarified to explain which outsourcing rules will prevail in the event of a conflict between DORA and sector-specific rules on outsourcing. On the requirement under DORA for critical ICT third-party service providers to be established in the European Economic Area, care is needed to strike the balance between, on the one hand, the risk such dependence might involve for financial institutions (either directly or via subcontracting) and, on the other hand, the risk of then no longer having access to certain ICT services.
- *Dedicated DORA oversight regime on critical ICT third-party service providers* – In the proposed oversight regime, it is key to foresee a more important role for the national competent authority of the Member State where the critical third-party service provider is established. Also, it will be more efficient and less costly to pool resources and expertise through centralisation of the Lead Overseer role at one ESA, rather than making all three ESAs responsible. Regarding the means of enforcement of (non-binding) recommendations made to critical third-party service providers, a comply-or-explain approach and an involvement of the Lead Overseer in the follow-up process to these recommendations is preferable. This will further ensure a coordinated and consistent approach across the Union. Furthermore, competent authorities of financial entities already interacting with critical ICT third-party providers used by entities under their supervision should be able to continue exercising their (prudential or other) powers with respect to these financial entities regardless of the (non-binding) recommendations issued under the oversight framework for critical third-party providers.

The Bank will continue to monitor how the DORA Regulation is further developed and how it can contribute to the successful implementation of this legislation within its current supervisory, oversight and policy-setting mandate.

Common observations from on-site inspections

As mentioned previously, a number of FMIs, PIs and ELMIs have in recent years been subject to on-site inspections focused on cyber and ICT risks. These activities frequently resulted in similar observations. Some of these thematic findings are summarised below.

In many cases, institutions still have room for progress in establishing sufficiently detailed and concrete strategies regarding security and continuity risks. Structured strategic reflection, decision-making and monitoring at board and senior management level is crucial here, as is sufficiently clear and comprehensive reporting on these risks and their evolution under the influence of mitigating measures and projects.

Institutions often still invest insufficient time and resources in their policy frameworks, including the related technical standards and procedures. This sometimes results in them not being sufficiently up to date, consistent, clear, feasible and/or adapted to the specific organisation.

Not all institutions have an adequate and sufficiently documented framework for managing ICT risks. This deficiency often impedes the performance of credible, standardised and sufficiently detailed risk assessments and prevents proper registration and monitoring of all identified risks.

In several cases, financial institutions were found to have insufficient resources or expertise or not to operate efficiently enough to manage and/or assess security-related risks appropriately. It is essential to avoid excessive fragmentation of responsibilities, but also to maintain the so-called three-lines-of-defence model for those institutions to which this applies.

Many institutions should still organise initiatives to make their staff aware of security risks more regularly, and monitor the effectiveness of these initiatives. Such initiatives should cover a wide range of topics and address all relevant target groups (board of directors, executive committee, end users, IT administrators, developers, etc.).

Furthermore, in order to properly define and prioritise controls, it is important that these institutions map their IT architecture, IT and data assets, interdependencies and associated communication flows in sufficient detail. However, it has been found that institutions often have only a partial overview of these elements. In addition, as mentioned earlier, it is crucial that institutions proactively identify which software is nearing the end of its life cycle, and take action in good time to avoid using software that is no longer supported by the supplier.

Some institutions should further improve their outsourcing and third-party risk policy frameworks and ensure that they are effectively implemented, in order to obtain a complete overview of the outsourcing on which they are dependent and of the controls that should mitigate the associated risks. This should also ensure, among other things, that all outsourcing contracts contain the necessary clauses and that important outsourcings are regularly audited.

Another frequent issue is the management, protection and monitoring of logical access rights. Particular attention should be paid to privileged access rights. Access to highly confidential and/or critical applications and administrator accounts should be protected by strong authentication solutions.

The resources provided for implementing and maintaining basic security controls and processes such as network segmentation, encryption, automated real-time detection of IT assets, vulnerability management, secure development practices, compliance monitoring, etc., are often still inadequate.

Solutions for detecting and responding to anomalous behaviour can often be further strengthened. In particular, the coverage of IT systems and applications, the intelligence used, the analytical capabilities to correlate different sources of information, the available response plans and resources, etc. are often in need of improvement.

Institutions should test their security and continuity measures and plans more regularly and in an integrated and representative manner, taking into account various extreme but plausible scenarios.

Finally, internal audit programmes sometimes do not yet sufficiently cover security and IT continuity risks. Institutions should also ensure that the resultant findings and recommendations are addressed as soon as possible.

Threat Intelligence-Based Ethical Red teaming in Belgium (TIBER-BE)

Samuel Goret

Technological progress leads to innovative possibilities and capabilities. Although it might enable you to get more things done in a day and simplifies complex tasks for users, the systems and infrastructure themselves are becoming increasingly complex. This added complexity entails all kinds of risks, and risks are where malicious actors see opportunities. The threat of bad actors capitalising on the risks incurred by ever ongoing change is only amplified by the existence of geopolitical tensions, bringing us to intent, goal, purpose or rather motive. If inequality, jealousy and greed are added to that mix, technology becomes a unique, fast and ever evolving playground for cutting-edge, highly adaptive and organised criminals, as well as nation state actors with a different worldview. In addition, there are the so-called "hacktivists" (cyber activists) or disgruntled employees (so called insider threat). Although the final goal of the various kind of actors listed above differs (disruption, financial gain, extortion or political objectives), they have all adopted technology as a new kind of weapon in a new kind of war. One might state that hacking is not a novelty, but the organised aspect of it has evolved at a rapid pace and can now be considered a business model. In contrast to conventional "defensive" security like firewalls, anti-malware tools, detection tools, SOC (Security Operation Centre), etc., offensive security tests the applications, systems and infrastructure from an attacker's point of view (including on-premises tests on physical security systems, like badge/access systems, or help desk staff through manipulative phone calls). This literally means acting as a bad actor and trying your best to get into the network, find the core critical systems and then demonstrate the capability to strike (in our case without really hitting the big red button). "To strike" could mean gaining financial benefit, exfiltrating trade secrets for later use, customer data, user credentials … or just encrypt all systems and cause major disruption for the FMIs or the economic system as a whole. This is the opposite of ethical hacking with its agreed rules of engagement, adherence to laws and high morality.

Fundamental principles of the TIBER-BE framework

Following the earlier implementations of the BoE's CBEST framework and DNB's TIBER-NL initiative, the ECB came up with a TIBER-EU framework for the European countries to implement, with varying degrees of freedom to consider the specificity of the local landscape. This harmonisation was duly needed as there was already a diverse range of tests at national level without clear guidelines for the financial institutions (FIs) and FMIs active on a pan-European scale. The NBB was the first NCB to customise the EU framework to better serve the Belgian concerned institutions (CI) and FMIs with headquarters in Belgium. It could thus reap the benefits of earlier work, while establishing a memorandum of understanding (MoU) for cross-jurisdictional collaboration, result- sharing and fostering mutual recognition of both the tests and the people involved. It should be highlighted that the TIBER framework is independent of the NBB's responsibility as prudential supervisor and overseer.

This is what *Threat Intelligence-Based Ethical Red teaming* (TIBER) is all about:

- *Threat Intelligence-Based* refers to analysing the global cyber security threat landscape with its current tactics, techniques and procedures (TTPs) used by real hackers, the current geopolitical landscape or the important events that change the way of working (e.g. COVID-19 pandemic leading to wide recourse to working from home). Threat intelligence (TI) has two major components: the *generic* threat landscape (GTL) investigates the cyber threat landscape from a financial sector's perspective. *Targeted* threat intelligence (TTI) focuses on the particular CI in scope, together with its distinct critical economic functions, infrastructure, staff, systems, software and processes.
- *Ethical* means the intent is to find relevant evidence, leading to concrete improvements and increased confidentiality, integrity and availability.
- *Red teaming* comes from the military exercises and simulation methodology where Red (attacker) vs Blue (defender) teams engage in realistic scenarios. In this kind of exercise, both the Red Team (RT) and the Blue Team (BT) start with minimal (grey box) to no information (black box) about each other's available intel, capability, techniques, tools or goals.

Performing TIBER-BE exercises

A typical TIBER tests consists of specific phases.

The first phase is the initiation and preparation phase serving to identify the major stakeholders. The *White Team* (WT) is a group of selected few of the CI knowing about the TIBER test. The *involved authorities* can vary greatly depending on the scope and often involve more NCBs in multi-country exercises, but the lead should always be with the NCB of the country where the headquarters of the CI resides. The *threat intelligence supplier* (TI) and the *Red Team supplier* (RT) are next to be identified. The choice of suppliers is such that it complies with all regulations and requirements of the involved authorities (e.g. CBEST and PASSI respectively UK and France). The suppliers should also have the required capabilities to effectively and efficiently provide return on investment and should vary sufficiently to broaden the types of approaches for simulated attacks. The last two stakeholders are the *Blue Team* (BT) and the *TIBER Cyber Team* (TCT). The BT is the existing defensive security organisation of the CI and is by design unaware of the existence, planning or any aspect of the TIBER test. The TCT consists of members of the authorities, mainly our NBB TIBER-BE test managers (their role is described in the box below).

BOX 14

The role of the TIBER-BE test manager

The typical tasks of a TIBER-BE test manager, key member of the TCT, are to:

- Provide insight into the GTL, together with the GTL supplier, as starting point of a TIBER project
- Guide the White Team through the TIBER process, methodology and deliverables to avoid pitfalls and provide maximum added value for the CI
- Act as catalyst and moderator between several stakeholders to ensure optimal collaboration, acting as a go-between and escalation point where needed, while ensuring confidentiality of the identity of the CI and the potential findings

- Be a neutral party but optimally use its sphere of influence during the whole process to keep the project on the rails, especially in the active testing phase and closure phase in order to mitigate any potential conflict of interests
- Deliver 360° feedback at the end of a test for all stakeholders as an opportunity to grow and learn for upcoming tests
- Analyse the lessons learnt from past tests to improve the TIBER-BE templates, guidelines and methodologies, whilst sharing experience with the TIBER-EU authorities (ECB, NCBs, etc.) and partners
- Discuss changes in the GTL on a pan-European level, with the involved parties and with its peers within the organisation.

During the second phase or test phase, with the GTL as starting point, the TI provider will firstly analyse the CI and its concrete threat landscape to generate the TTI and, secondly, the RT supplier will execute the selected realistic scenarios in a red-teaming setting, in accordance to the CI's risk appetite. This is by far the longest part of the project, with periods where the RT tries to execute the scenarios, with some "lay-low" periods to avoid detection and periods of fast decision-taking to take advantage of limited windows of opportunity. The action taken in this phase and the findings (e.g. the Red Teaming test summary) are strictly confidential.

The final phase or closure phase will provide an opportunity for all involved parties to learn and improve. This is done by re-playing the attack together with the BT and the RT (the so-called Purple teaming or PT), by agreeing on a remediation plan and sharing feedback between the institution, the suppliers, the TIBER team and other involved authorities in the form of a 360° evaluation, led by our TCT.

TIBER-BE is distinct from other Red Team penetration tests. For example, should the RT be blocked in a certain scenario, for instance because the CI's defence capabilities are successfully detecting and stopping every phishing attempt, there is the possibility of using a "leg-up". A leg-up bypasses the current roadblock and enables the Red Team to continue its work as if the intermediate step, in the above example the phishing, would have been successful. Such a leg-up can, for example, be providing direct network access, valid credentials or additional insight into technology to help the Red Team advance and make sure the TIBER exercise still has the best possible added value.

Another aspect is that, on top of the planned scenarios, there is the possibility of building a scenario "X" as the project evolves. In this special scenario, unexpected yet interesting findings, can be leveraged to make fully use of the suppliers' TI and RT capabilities in order to reach the most critical systems and thoroughly test the cyber defences of the CI, from an angle that might be very different than the usual TTP's of currently identified threat actors. This mimics potential future threats.

Continuously improving the TIBER Framework and perspective

To boost collaboration with the CIs within the TIBER-BE sphere of influence, the NBB organises and leads the TIBER National Implementation Committee (NIC). This makes it possible for CIs and suppliers to discuss their experience and for the NBB to boost the involvement of the different partners. No specificities can be shared during meetings of this forum, but this makes it even more interesting to analyse the high-level findings and

share recommendations on both cyber resilience and TIBER methodology in order to understand the emerging patterns and how to implement improvements for the whole financial sector. After all, TIBER is not about implementing a certain patch against a certain vulnerability, or even about generic pattern findings like top ten cyber security risks. It is about choosing the right organisational, methodological and systemic continuous improvements that provide the highest value added considering the real and recently emerging cyber threats. One of the main focus is to test the capabilities of the Blue Team. Although individual test results are strictly confidential, a few insights into identified issues and risks can be shared, as these are well known to bad actors and not characteristic of the financial sector, while understanding that the risks and high-value targets remain distinctive, the sector can still benefit from improving generic defences. Network access control (NAC or network segregation) is not always correctly implemented in all parts of the network, making pivoting and lateral movement from a low-value target or machine to a high value one "relatively" easy for a skilled hacker. Another pattern that can be identified is the hard-shell syndrome: it is hard to get into the institution given decent perimeter defences, both logical (websites, end-user devices and virtual private networks) and physical (doors, locks, security cameras) are well-established, guarded and monitored. But once a malicious actor has gained access to the internal network, there are fewer barriers in place to prevent privilege escalation, exfiltration of confidential data or breach critical systems without being detected. It is worth noting here that a substantial degree of compromise come from insider threats, actors that are already inside the network or even employees. Using decoys (also known as honeypots and canaries) is another good practice that is not used to its full potential yet. Extending and refining the granularity of defence mechanisms inside the core network, as well as implementing multi-layer detection capabilities is thus paramount to a modernised cyber resilience.

From past experience, the TIBER-BE team could already draw some interesting lessons. One attention point is refining the so called Purple Teaming phase: scenario replay, cooperative red-teaming, simulation, knowledge-sharing and instating the right mindset to make sure the Red and Blue Teams act as one, with the same final objective in mind, namely raising the CI's detection and response capabilities. Another point of focus is sharing results with regulators without endangering the CI, whilst ensuring that the remediations are put in place correctly and in good time. Some CIs are already top of the class and the usual mimicking of current bad actors will not help learn any new lessons since all known threat actor *modus operandi* (MOs) are detected and mitigated instantaneously. For these mature institutions, one could consider putting scenario "X" first to increase the return on investment of the TIBER exercise. Certain red-teaming activities involve trying to physically gain unauthorised access to a company's assets. The coronavirus pandemic poses a serious challenge for this kind of test as access control is tightened and it is not easy to blend in if only a few people are present on the premises. This also poses difficulties for the other parties involved in the test, as it is challenging to securely exchange highly confidential documents that are normally only to be consulted on site. It should also be highlighted that the upcoming Digital Operations Resilience Act (DORA) will potentially increase the current scope and may change the flexibility and freedom of action of the framework. This might also have an impact on the three-year cycle, potentially reducing the effectiveness of the methodology. Moreover, globalisation and the growing international dimension beyond the EU increase the difficulty of correctly managing expectations and ensuring an optimal outcome, for a realistic effort and feasibility.

In addition, the growing outsourcing to Software as a Service (SaaS), cloud or other specialised third parties affects diverse aspects such as scope, legality and responsible disclosure. TIBER intends to test the CI, not the SaaS providers. The test also needs to respect the terms of service of parties that are in fact not part of the test but hosting the CI's services. The recent shift towards agile project methodology can in some cases also result in paying less attention to non-functional requirements, in this case security aspects. Recent and rapidly evolving internet-facing technologies (cloud, blockchains, Internet of Things, mobile, artificial intelligence, robotic process automation) extends the attack surface and yields unfamiliar attack vectors and experimental TTPs. Malicious actors have at the same time boosted their deceptive capabilities. Finding suppliers with the skills to understand and mimic these innovative TTPs is hard. There is a scarcity of skilled RT providers in the EU, given that including non-EU providers involves supplementary challenges and risks, such as data safe-haven questions, General Data Protection Regulation and geopolitical implications and certification recognition. Finally, recent incidents in cyber security point out the steep rise in supply-chain types of attack, targeting the weakest link in a supply chain to

compromise assets very early on. A simple example is tampering with ATMs during the manufacturing phase long before they are shipped to a bank instead of trying to attack ATMs that are already installed. A more complex example might be to compromise code compilers used to produce software that is later used to push certificates from a trustworthy source to banking application users. In other words, the security of a company is as good or rather as weak as the weakest link in all its combined supply chain components as malicious actors take the path of least resistance, not necessarily the most obvious one.

The feedback from the various involved institutions after the first TIBER tests so far is very positive. The sector appears to be convinced of the methodology and the added value of this opportunity to raise cyber security awareness, gain valuable insight into present and future threats, improve intrusion detection/protection capabilities and cyber resilience in the broader sense. All of which is contributing to higher confidentiality, integrity and availability with the final goal being to improve financial stability, in line with the NBB's key mission.

FMI-PSP Inspections

Hilal Sefsaf and Jozefien Uytterhoeven

FMI-PSP inspection team purpose

At the end of 2018, the Board of Directors of the NBB decided to set-up a cell of inspectors specifically dedicated to the on-site inspections of payment institutions, financial market infrastructures and critical operators (namely FMI-PSP Inspections).

The decision to reinforce the coverage of these entities through on-site inspections is based on several considerations, explained hereafter, and has for objective to ensure the operational stability and resilience of the sector. The first consideration involves the growing number of licensed payment institutions (PIs) and electronic money institutions (ELMIs) in Belgium, also due to Brexit, which present a wide range of degree of maturity in their organisation. Secondly, the prudential framework these entities have to comply with is composed of a wide range of requirements necessitating a specific team to understand these and practically observe how the institutions implement them. Thirdly, the diversity of activities and systems used by these entities results in specific risks that can vary materially in nature, origination, and manifestation, which may lead to some of them presenting a high-risk profile.

So, the inspection team FMI-PSP was set up in the course of 2019 with the goal of raising the visibility on these entities, by carrying out inspections on the non-banking framework with which the PIs, FMIs and critical operators have to comply. The non-banking framework includes notably the Directive 2015/2366 on Payment Services (PSD2), the Principles for Financial Market Infrastructures (PFMI), the Regulation 909/2014 on settlement and central securities depositories (CSDR) and the Regulatory Technical Standards (RTS) provided by ESMA and EBA, the Directive 2002/47/EC on financial collateral arrangements, the Directive 98/26/EC on settlement finality in payment and securities settlement systems (SFD), the CPMI-IOSCO guidance on recovery on financial market infrastructures, the Law of 24 March 2017 on the oversight on payment transaction processors, and Circular PPB-2007-7-CPB on the administration on financial instruments.

The FMI-PSP inspections can be thematic, on specific requirements of the non-banking framework, or so called "event-driven" when specific needs arise. The inspection team performs planned examinations in order to get positive assurance about compliance with regulatory requirements and detect potential deficiencies or possible improvements and best practices (for example, with regard to a cross-sectoral benchmarking). When necessary and relevant, the inspection team can also collaborate with other NBB inspectors, such as IT or AML inspectors, for a joint inspection.

FMI-PSP inspection approach in 2020

Over the course of 2020, the FMI-PSP Inspection team developed an inspection methodology in line with the Circular NBB_2013_15 on NBB inspections, as well as a risk-based model to determine a risk score per institution,

in order to prioritise inspections according to a risk-based approach. The inspection team put together a control matrix that translates the regulatory framework into specific controls and is used to draw up work programmes and carry out on-site inspections.

During 2020, the inspection team focused on PIs and ELMIs due to the numerous challenges observed in the sector such as the implementation of PSD2 and SCA requirements, the high number of newly licensed institutions, and the institutions that relocated to Belgium as a consequence of Brexit. Several thematic inspections were therefore launched on general governance requirements and the safeguarding principle, a core element of PSD2, in order to ensure the protection of client funds.

Regarding governance, the inspections aimed to ensure that incoming institutions, as a consequence of Brexit, were not just "empty shells". As the PSD2 implementing Law of 11 of March 2018 requires, the inspections specifically checked whether the effective management is composed of two effective leaders, physical persons, and/or that the effective leader role is sufficiently executed, formalised and assessed. Furthermore, it was ensured that the management bodies are adequately structured and systematically perform the duties that fall under their function (e.g. annually assessing the compliance function). Finally, it was systematically assessed whether the central administration could be considered as located in Belgium, based on the above attention points and additional evidence demonstrating that decisions are taken and implemented locally, particularly in the context of a group. The review of the accounting and administrative organisation was included in the assessment of the central administration, particularly with respect to the management of the internal documentation, the financial reporting process and the communication of significant changes and breaches to the regulator.

In regard to the independent control functions in place, the inspections focused on the independence of the three lines of defence and on the effective execution of their duties.

As far as outsourcing is concerned, several inspections assessed the adequacy of the formalisation of both the outsourcing framework and monitoring of the outsourced activities, particularly in the context of intra-group outsourcing.

Finally, regarding the protection of clients' funds (i.e. the safeguarding principle), the inspections verified whether the entities complied with the formal requirements including the use of segregated accounts[1]. Furthermore, the operational risk on the safeguarding and reconciliation processes, as well as the internal controls system in place on these processes, were systematically reviewed to ensure that the formalisation of both the controls and the procedures were adequate, as well as the independence of the control function and the regulatory mandatory reporting.

FMI-PSP inspection priorities in 2021

The FMI-PSP inspection team has established a risk-based inspection plan for the years to come and the inspection programme for 2021 is the continuation of the 2020 programme. Accordingly, the inspection team will pursue inspections at PIs and ELMIs on core elements of the PSD2 Law such as the safeguarding requirements, as well as pay close attention to the institutions recently transferred to the NBB's supervision as a consequence of Brexit, particularly in terms of governance (e.g. central administration). Furthermore, the inspections' scope will extend to other infrastructures, such as FMIs, as foreseen in the mandate.

1 As specified in the Law of 11 March 2018: Articles 41 and 42 for PI and Article 194 for ELMI.

Annexes

Annex 1: Regulatory framework

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

CCPs	**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. https://eur-lex.europa.eu/eli/reg/2019/834/oj
	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. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R2099
	CPMI-IOSCO Public quantitative disclosure standards for CCPs (February 2015): Public quantitative disclosure standards that CCPs are expected to meet. These standards complement the Disclosure framework published by CPMI-IOSCO in December 2012. http://www.bis.org/cpmi/publ/d125.pdf
	EMIR Regulatory Technical Standards (August 2015): Regulation (EU) 2015/2205 of 6 August 2015 supplementing Regulation (EU) No. 648/2012 with regard to regulatory technical standards on the clearing obligation. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R2205&from=EN
	CPMI-IOSCO Resilience of CCPs: Further guidance on the PFMI (July 2017): Guidance providing further clarity and granularity on several key aspects of the PFMI to further improve CCP resilience. https://www.bis.org/cpmi/publ/d163.pdf
	Regulation on CCP recovery and resolution: Regulation (EU) 2021/23 of the European Parliament and of the Council of 16 December 2020 on a framework for the recovery and resolution of central counterparties and amending Regulations (EU) No 1095/2010, (EU) No 648/2012, (EU) No 600/2014, (EU) No 806/2014 and (EU) 2015/2365 and Directives 2002/47/EC, 2004/25/EC, 2007/36/EC, 2014/59/EU and (EU) 2017/1132, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2021:022:TOC

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

Payment Systems	**ECB Regulation (EU) No 795/2014 on oversight requirements for systemically important payment systems (July 2014):** Regulation, based on the CPMI-IOSCO PFMIs, covering systemically important payment systems in the eurozone, large-value and retail payment systems. https://www.ecb.europa.eu/ecb/legal/pdf/oj_jol_2014_217_r_0006_en_txt.pdf
	Revised oversight framework for retail payment systems (RPS) (February 2016): Revised framework (replacing the one from 2003) identifying RPS categories and clarifying the oversight standards applicable to each category. It also provides guidance on the organisation of oversight activities for systems of relevance to more than one central bank. https://www.ecb.europa.eu/pub/pdf/other/revisedoversightframeworkretailpaymentsystems201602.en.pdf?bc332d9a718f5336b68bb904a68d29b0
PIs & ELMIs	**EMD2 (September 2009):** Directive 2009/110/EC of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of ELMIs amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC, OJ. 10 October 2009, L. 267, 7-17. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0110&from=EN
	PSD2 (November 2015): Directive (EU) 2015/2366 of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015L2366
	Belgian Law of 11 March 2018 transposing the PSD2, Belgian Official Gazette 26 March 2018. https://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=2018031107&table_name=wet/language=fr&la=F&cn=2018031107&table_name=loi
Payement Processors	**Belgian Law of 24 March 2017 on supervision of payment transactions processors,** *Belgian Official Gazette* 24 April 2017. https://www.nbb.be/doc/cp/moniteur/2017/20170424_opp_wet_loi.pdf
	Royal Decree of 8 February 2019 on the requirements for processors of retail payments instruments and card payments schemes (CPS) having established a relation with them on the due diligence that CPS must have in place when using the services of systemically relevant payment processors, the identification and management of the risks by those processors, the continuity of their services and the practical modalities of the communication in case of an incident. http://www.ejustice.just.fgov.be/eli/arrete/2019/01/25/2019030120/moniteur **(FR) or** http://www.ejustice.just.fgov.be/eli/besluit/2019/01/25/2019030120/staatsblad **(NL)**

Card Payment Schemes	**Eurosystem Oversight Framework for Card Payment Schemes (CPSs) – Standards (January 2008):** Common oversight policy to promote the reliability of CPSs operating in the euro area, public confidence in card payments and a level playing field across the euro area in a unified market. https://www.ecb.europa.eu/pub/pdf/other/oversightfwcardpaymentsss200801en.pdf
	Guide for the assessment of CPS against the oversight standards (February 2015): Assessment guide based on the Eurosystem Oversight Framework for CPSs targeting both governance authorities responsible for ensuring compliance and overseers of CPSs It has been updated by taking into account the January 2013 "Recommendations for the security of internet payments", as well as the February 2014 "Assessment guide for the security of internet payments". https://www.ecb.europa.eu/pub/pdf/other/guideassessmentcpsagainstoversightstandards201502.en.pdf?499089f7f3aab273925ef6d80767b4a5
	Regulation (EU) 2015/751 of 29 April 2015 on interchange fees for card-based payment transactions (OJ. 19 May 2015, L. 123, 1-15): This regulation contains (i) the definition of a cap for the interchange fees applicable to payment transactions by means of debit or credit cards, (ii) the separation to be put in place between payment card scheme governance activities and processing activities, (iii) measures granting more autonomy to merchants regarding the choice of payment instruments for their clients. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R0751&from=EN
	Belgian Law of 1 December 2016 transposing the EU Regulation 2015/751 of 29 April 2015, entitled "Interchange fees for card based payment transactions" (December 2016): *Belgian Official Gazette* 15 December 2016, 86.578. https://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=2016120112&table_name=wet/language=fr&la=F&cn=2016120112&table_name=loi
	Regulation (EU) 2018/72 of 4 October 2017 supplementing Regulation (EU) 2015/751 on interchange fees for card-based payment transactions with regard to regulatory technical standards establishing the requirements to be complied with by payment card schemes and processing entities to ensure the application of independence requirements in terms of accounting, organisation and decision-making process OJ. 18 January 2018, L. 13/1-7. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R0072&rid=3

SWIFT	**High level expectations (HLE) for the oversight of SWIFT (June 2007):** The SWIFT Cooperative Oversight Group developed a specific set of principles that apply to SWIFT. https://www.nbb.be/en/financial-oversight/oversight/critical-service-providers#oversight-of-swift-
	PFMIs, Annex F: Oversight expectations applicable to critical service providers (April 2012): Expectations for an FMI's critical service providers in order to support the FMI's overall safety and efficiency. https://www.bis.org/cpmi/publ/d101a.pdf
	Assessment methodology for the oversight expectations applicable to critical service providers (December 2014): Assessment methodology and guidance for regulators, supervisors and overseers in assessing an FMI's critical service providers against the oversight expectations in Annex F. https://www.bis.org/cpmi/publ/d123.pdf

Annex 2: FMIs established in Belgium with an international dimension

Euroclear

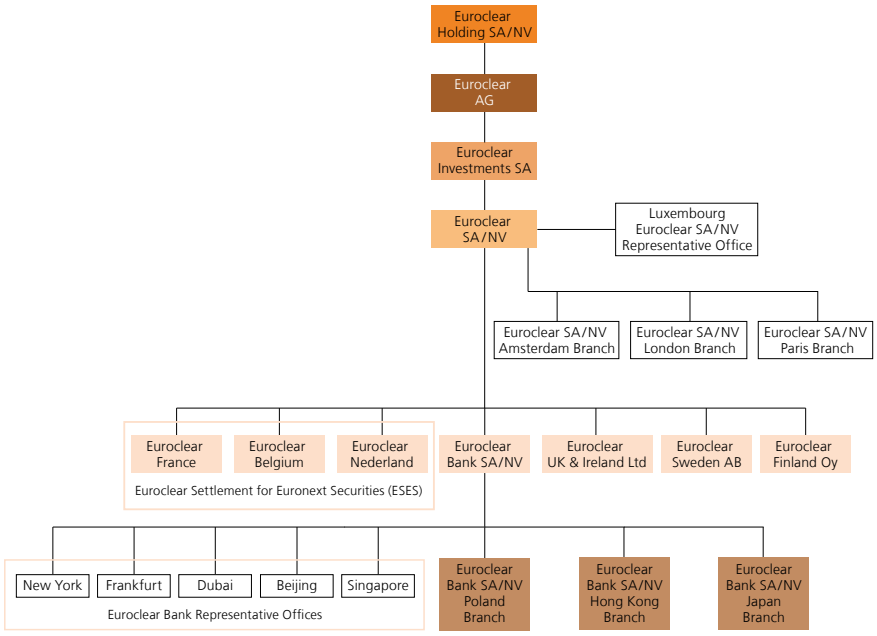
Euroclear Holding SA/NV, the top financial holding of Euroclear, is incorporated under Belgian law. Euroclear. Holding SA/NV owns 100 % of Euroclear AG, a Swiss financial holding company. Euroclear Investments SA is the group's financial investment holding company, incorporated in Luxembourg.

Euroclear SA/NV (ESA), a Belgian financial holding company, is the parent company of the Euroclear Group (I) SDs; 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.

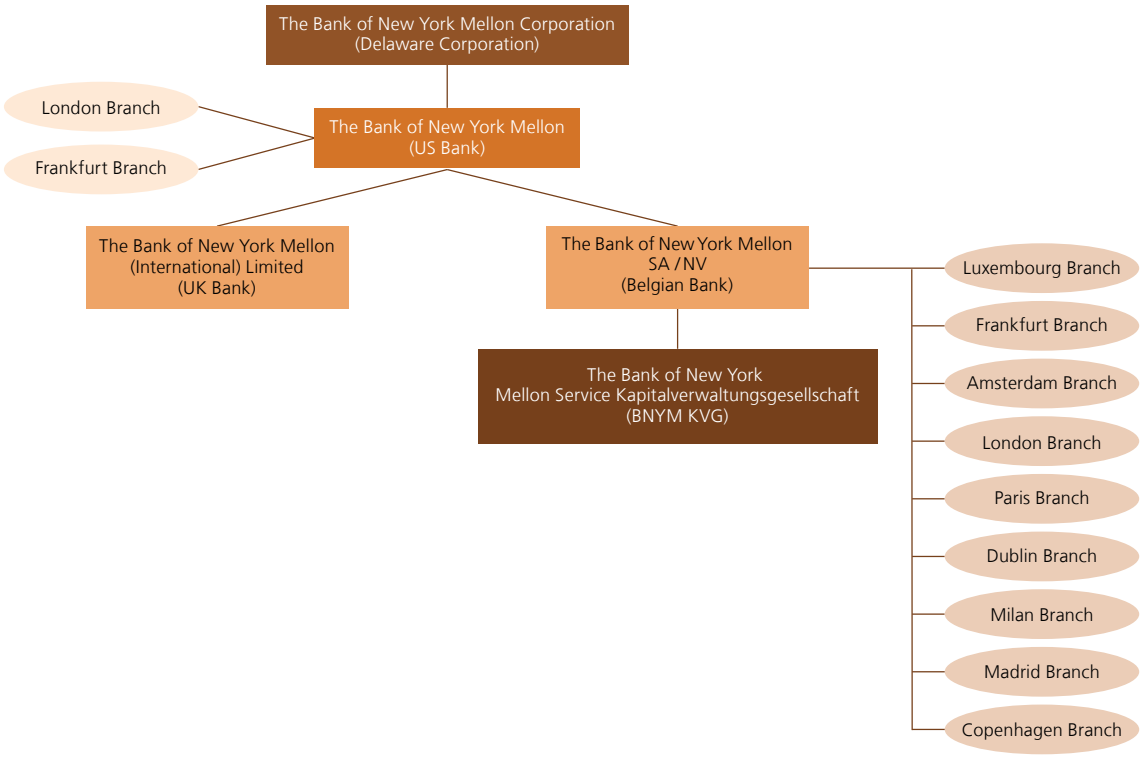
The Bank of New York Mellon

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, Italy, Spain and Denmark 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: BNY Mellon.

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.

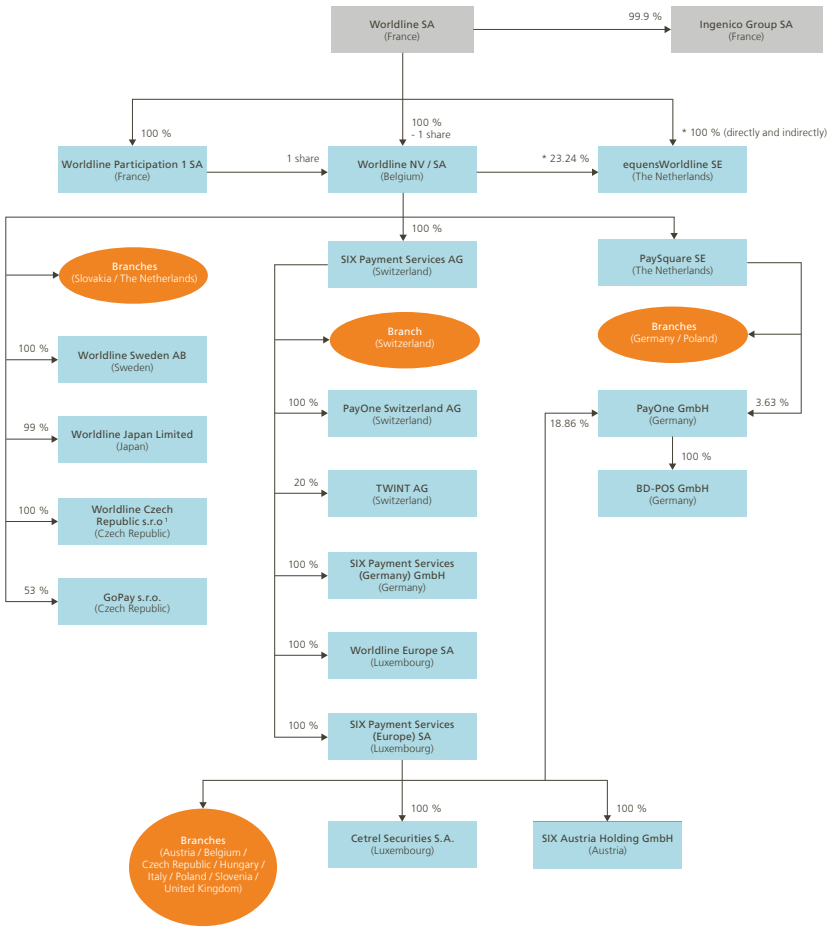
In 2016, Worldline SA/NV, the Belgian entity of the group merged with the Dutch company Equens. The processing activities were carved out in a new entity called equensWorldline SE. equensWorldline SE is now a full subsidiary of Worldline SA (France).

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). After the acquisition of Ingenico, Worldline became the largest European provider of payment services.

Chart 3

Structure of Worldline

(as of 1 April 2021 – after absorption of Worldline BV, simplified diagram, part of the group relevant for Belgium)



Source: Worldline.

* The remaining 1 % is held by Komercni Banka. The voting rights held by Worldline NV/SA amount to 60 %. The remaining voting rights are held by Komercni Banka.

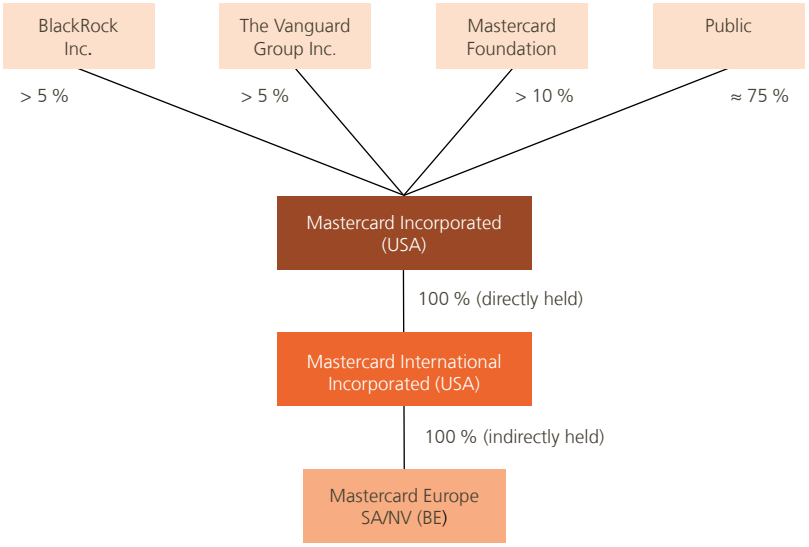
Mastercard Europe

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 2021)



Source: Mastercard Europe.

Annex 3: Statistics

List of tables

Table 1

Securities Clearing, Settlement and Custody

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

	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
A. Central Counterparties (CCPs) (selected)										
LCH Ltd (UK)										
Repos (all currencies combined)	93 331	84 108	79 245	78 118	79 300	77 039	87 553	89 822	44 795	
LCH SA (FR)										
Credit Default Swaps (all currencies combined)	62	91	336	123	346	898	1 098	1 225	1 517	
Repos (Belgium, all currencies combined)	701	985	1 341	1 567	1 345	1 259	890	1 128	2 503	
Eurex Clearing AG (DE)										
Repos (all currencies combined)	20 210	16 838	20 858	28 953	22 251	12 084	9 025	11 299	14 722	

Source: ECB Central Counterparty Clearing Statistics.

Table 1 (continued)

Securities Clearing, Settlement and Custody

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

	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
B. Euroclear Bank										
Value of securities deposits (end of period)	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	15.292.4
Number of transactions (in millions)	59.4	64.2	69.5	75.2	83.3	84.1	95.4	107.0	116.4	128.8
Value of transactions	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	575.991.9
Source: Euroclear.										
C. NBB-SSS										
Value of securities deposits (end of period)	513.3	531.2	541.7	557.3	575.4	612.5	625.3	632.6	646.65	698.66
Number of transactions (in millions)	0.5	0.6	0.6	0.6	0.5	0.5	0.5	0.5	0.5	0.5
Value of transactions[1]	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	9 220.7
Source: NBB. 1 Secondary market turnover.										
D. Euroclear Belgium										
Value of securities deposits (end of period)	130.4	156.8	202.7	222.1	269.4	235.1	237.7	178.0	220.2	194.9
Number of transactions (in millions)	1.9	1.9	1.9	2.1	2.5	2.4	2.5	2.7	2.6	2.9
Value of transactions	588.0	563.6	799.8	714.8	944.6	963.8	946.0	964.1	783.9	704.9
Source: Euroclear.										
E. TARGET2-Securities[1]										
Number of transactions (in millions)	nap	nap	nap	nap	7.6	36.3	125.6	145.9	154.8	176.7
Value of transactions	nap	nap	nap	nap	43 706.8	112 066.0	192 175.0	236 050.8	282 063.7	172 840.9
Source: ECB. T2S was launched in 2015. 1 As of 2020, the values in this table excludes technical transactions in T2S and liquidity transfers from traffic statistics.										
F. BNYM SA/NV										
Value of assets held under custody (end of period)	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	2 903.5
Source: BNYM.										

Table 2

Payments

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

	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
A. TARGET2										
Value of payments	651 274.9	711 025.8	559 696.0	498 726.5	508 982.3	485 811.8	432 780.7	432 508.1	441 281.1	465 793.7
of which : TARGET2-BE	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	28 570.6
Number of payments (in millions)	89.0	89.6	91.3	87.8	88.6	89.0	89.3	88.4	87.8	88.7
of which : TARGET2-BE	2.6	2.5	2.3	2.5	2.3	2.2	2.3	2.3	2.5	3.1
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										
Value of payments (in € trillion)	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	1 335 152.0
of which : EUR payments	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	244 744.0
Number of payments (in millions)	206.9	176.6	205.0	204.7	219.1	209.5	198.5	226.6	257.1	273.5
of which : EUR payments	45.5	37.4	36.9	34.4	40.9	34.3	34.0	39.1	42.2	45.4
Sources : ECB Payment Statistics, CLS.										
C. Centre for Exchange and Clearing (CEC)										
Value of payments (exclusive Instant Payments since 2020 [1]) (in € billion)	886.7	909.1	911.6	870.7	883.4	920.6	941.8	1 122.9	1 204.7	1 198.8
Value of Instant Payments (in € billion)	nap	nap	nap	nap	nap	nap	nap	nap	nap	57.2
Number of payments (exclusive Instant Payments since 2020 [1]) (in millions)	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	1 396.9
Number of Instant Payments (in millions)										99.6
Sources : ECB Payment Statistics, CEC.										
1 As of 2020, data on Instant Payments is reported separately.										

Table 2 (continued 1)

Payments

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

	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
D. Payment Institutions (PIs) – Electronic Money Institutions (ELMIs)										
PIs										
Belgian PIs	9	9	11	15	17	21	24	22	26	30
Account information services providers									1	3
Foreign PIs with Belgian branch	0	2	2	3	3	3	2	3	4	5
Passport notifications for cross-border services										
Belgian PIs towards other EEA countries	19	19	26	41	65	162	218	248	440	435
Foreign EEA PIs towards Belgium	104	133	184	262	273	379	421	435	511	566
ELMIs										
Belgian ELMIs	6	6	10	10	10	8	8	7	7	7
Foreign ELMIs with Belgian branch	0	0	0	1	1	1	1	2	1	1
Passport notifications for cross-border services										
Belgian ELMIs towards other EEA countries	18	19	43	45	69	70	72	72	104	104
Foreign EEA ELMIs towards Belgium	14	28	40	54	53	102	156	188	240	278
Institutions offering services within a limited network (new under PSD2)								1	4	5
Transactions by Belgian PIs and ELMIs (in millions)										
Number of transactions (yearly total)	nav	nav	1 665	1 874	1 968	2 155	2 006	2 044	1 949	2 106
Value of transactions in euro (yearly total)	nav	nav	105 989	133 513	136 567	137 144	124 388	124 485	113 639	121 751
Average outstanding E-Money of Belgian ELMIs	nav	nav	15.2	21.8	35.8	45.5	73.9	116.6	405.2	494.3
Source : NBB.										
E. Processors of payment transactions										
Worldline SA/NV										
Number of transactions (yearly total, in millions)[1]	1 387.6	1 473.7	1 553.9	1 665.8	1 800.0	1 960.0	2 150.0 1 746	1 774	1 940	1 972
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

	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
F. Card transactions										
Number of cards issued by resident payment service providers – Cards with a cash function										
Number of cards (in thousands, end of period)				21 396.5	21 875.0	22 593.1	22 537.8	23 904.7	35 186.9	nav
Number of cards per capita (end of period)				1.9	1.9	2.0	2.0	2.1	3.1	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	78.2	73.7	44.3	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	3 739.6	3 189.8	1 848.9	nav
Transactions per capita										
Number of card payments – With cards isssued by resident PSPs [1] (yearly total)				135.2	130.9	149.5	158.5	183.0	204.1	nav
Value of card payments – With cards issued by resident PSPs [1] (yearly total, in € thousands)				7.2	7.4	8.1	8.2	8.5	9.1	nav
Source : ECB Payment Statistics.										
1 Except cards with an e-money function only.										
G. Card schemes										
Bancontact – Number of transactions (yearly total, in millions)	1 076.4	1 136.4	1 180.4	1 241.8	1 306.7	1 389.5	1 441.6	1 480.2	1 593.4	1 706.1
of which :										
Retail payments	973.4	1 028.9	1 068.4	1 125.9	1 190.9	1 272.8	1 325.2	1 336.0	1 488.8	1 637.5
ATM	103.0	107.5	111.9	115.9	115.9	116.8	116.3	114.2	104.6	68.6
Source : Bancontact.										

Table 3

SWIFT

(yearly total, in millions)

	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
Number of messages	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	9 526.5
of which:										
Payment messages	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	4 313.0
Securities messages	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	4 709.8
Other messages	330.5	299.4	325.6	330.3	347.3	367.3	359.0	398.1	432.1	503.8

Source: SWIFT.

List of abbreviations

AISP	Account information service provider
AML/CTF	Anti-Money Laundering / Combating the Financing of Terrorism
API	Application programming interface
ART	Asset-referenced token
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
CBDC	Central bank digital currency
CCP	Central counterparty
CEC	Centre for Exchange and Clearing
CLS	Continuous Linked Settlement
CMG	Crisis Management Group
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
DLT	Distributed Ledger Technology
DORA	Digital Operational Resilience Act
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
EMT	Electronic money token
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
IBAN	International Bank Account Number
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
LSI	Less significant institution
LVPS	Large-Value Payment Systems
MCE	Mastercard Europe
MCMS	Mastercard Clearing Management System
MiCA	Markets in Crypto-Assets
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
PISA	Payment instruments, schemes, and arrangements
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

Dominik Smoniewski
Head of
Surveillance of financial market infrastructures, payment services
and cyber risks

Tel. +32 2 221 20 57
dominik.smoniewski@nbb.be

Cover and layout: NBB CM – Prepress & Image

Published in June 2021

Printed on FSC paper