Financial Market Infrastructures and Payment Services Report 2023

National Bank OF BELGIUM
Eurosystem

Financial Market Infrastructures and Payment Services Report 2023

National Bank OF BELGIUM
Eurosystem

Contents

Executive summary

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

Digital operational resilience

In order to guarantee financial stability, these critical institutions need to manage their operational risks – including IT and cyber risks – very carefully. Digital operational resilience was therefore one of the Bank's top priorities again in 2022. The Bank is not the only regulator focusing on this risk. In that context, the Bank's staff actively contribute to various policy initiatives. In March 2021, the Basel Committee on Banking Supervision published new principles for strengthening the operational resilience of banks, including a specific focus on ICT and cyber security. At EU level, the Digital Operational Resilience Act (DORA) entered into force on 17 January 2023. Its provisions aim at mitigating the risks associated with the digital transformation of the financial industry by imposing strict common rules. These rules apply to a wide range of financial institutions, plus critical IT third-party service providers, for example cloud service providers, who would be subject to a form of EU oversight. A thematic article on digital operational resilience also includes some observations from recent on-site IT inspections.

The increased use of technology does not only create risks, it also provides business opportunities for some entities. Emerging technologies such as distributed ledger technology (DLT) are closely monitored by the authorities to assess their potential impact on financial stability. The EU's Markets in Crypto-Assets Regulation (MiCA), for example, seeks to ensure a level playing field for consumer protection, market integrity, financial stability, monetary policy transmission and monetary sovereignty. In October 2021, with these concerns in mind, the Eurosystem started the investigation phase on the subject of a central bank digital currency (CBDC); by the end of 2023, more should be known about whether we move on to the next stage and what it would look like.

The Russian invasion of Ukraine

Over the course of 2022, the Bank closely monitored the impact of the geopolitical crisis as a result of the Russian invasion of Ukraine. Since the Russian invasion, several countries have imposed sanctions on Russian organisations and citizens. Those sanctions, as well as the Russian countermeasures, had an impact on some of the institutions that are subject to the National Bank of Belgium's oversight and supervision.

Environmental and climate-related risks

Environmental and climate-related risks are another type of risk that has been receiving more and more attention at the Bank and in the wider community. While market infrastructures may not be exposed to climate risk in the same way as, for example, insurers that insure damage caused by extreme weather events, companies active in custody, payments and financial messaging need to manage this type of risk carefully as well. One of the

environmental and climate-related risk categories identified by all entities covered by this Report is physical risk from natural disasters, and extreme weather events interrupting the services delivered by the institution itself or by one of its service providers. Moreover, just as Swift acts as a facilitator to enhance its clients' cyber security with its Customer Security Programme (CSP), institutions in the custody, payments and financial messaging sectors believe that they can play a positive role in helping the financial community tackle environmental and climate-related risks, in addition to reducing their own CO2 emissions. A dedicated thematic article provides an update of the previous article on environmental and climate-related risks within the FMI landscape.

Oversight and supervision activities

In addition to the ongoing supervision and annual assessments, the Bank keeps an eye on major changes, such as the introduction of the CSDR settlement discipline regime for CSDs, the designation of Wordline Switzerland Ltd as a systemically important payments processor for the Bancontact scheme, or Swift's migration from the FIN MT standard to the ISO 20022 MX standard for financial messaging.

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

To give 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 presents an overview of their structure and mutual interdependencies. Relevant processes and flows are explained in more detail in the subsequent parts of this report (i.e. chapters 2, 3 and 4). Section 1.2 explains the Bank's mandate and its role in the oversight and prudential supervision of this sector, from either a national or an international perspective.

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

The systems and institutions covered in this report can be divided into three categories according to the type of service provided: (i) securities clearing, settlement and custody, (ii) payments, and (iii) other financial infrastructure service providers. Through their activities or services for the financial industry, these systems and institutions are the critical links in the functioning of financial markets and payment services, and in 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 instruments can take place 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 may 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 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 CCP's direct participants – usually banks or

investment firms – are called clearing members. A clearing member may clear not only its own trades via the CCP, but also those of its clients. There are no CCPs established in Belgium, but CCPs in other countries are important for Belgium 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 a financial instrument between the parties in the books of a central securities depository (CSD). When a CCP has intervened to clear a trade, settlement takes place on the books of the CSDs between the buyer and the CCP, and between the seller and the CCP. There are three CSDs established in Belgium: Euroclear Bank (an international CSD or ICSD), Euroclear Belgium and NBB-SSS (both CSDs). The settlement of the cash leg of securities transactions takes place either in payment systems operated by central banks (i.e. central bank money, for example T2[1]) 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 intermediary capacity, 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 payments (i.e. transactions between banks for institutional investors) and retail payments (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 very large amounts, 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 T2, the LVPS connecting Belgian banks 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 multi-faceted and growing. PIs and ELMIs have long been active in the card payment business, issuing payment cards to users and/or acquiring the funds for payments on behalf of merchants. The revised 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. In a transaction with a merchant, the card of the purchaser (cardholder) is issued by an institution (card issuer) which was traditionally always a bank but can also be a PI or ELMI. The acquirer is in charge of acquiring the transaction on behalf of the merchant (i.e. performing for the merchant all the steps necessary for the buyer's money to be paid into the merchant's account). The 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.

1 As of 20 March 2023, the new payments system T2 went live and replaced TARGET2. For more detailed information, see https://www.ecb.europa.eu/press/pr/date/2023/html/ecb.pr230321~f5c7bddf6d.en.html.

As from May 2020, the Eurosystem designated MCE as a systemically important payment system (SIPS) according to the ECB SIPS Regulation criteria. The Mastercard Clearing Management System operated by MCE has become the fifth SIPS in the euro area, alongside T2, EURO1, STEP2 and CORE-FR. For the first time, an entity active in the card business has been designated as a SIPS; its business activities stem exclusively from 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 also play 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.

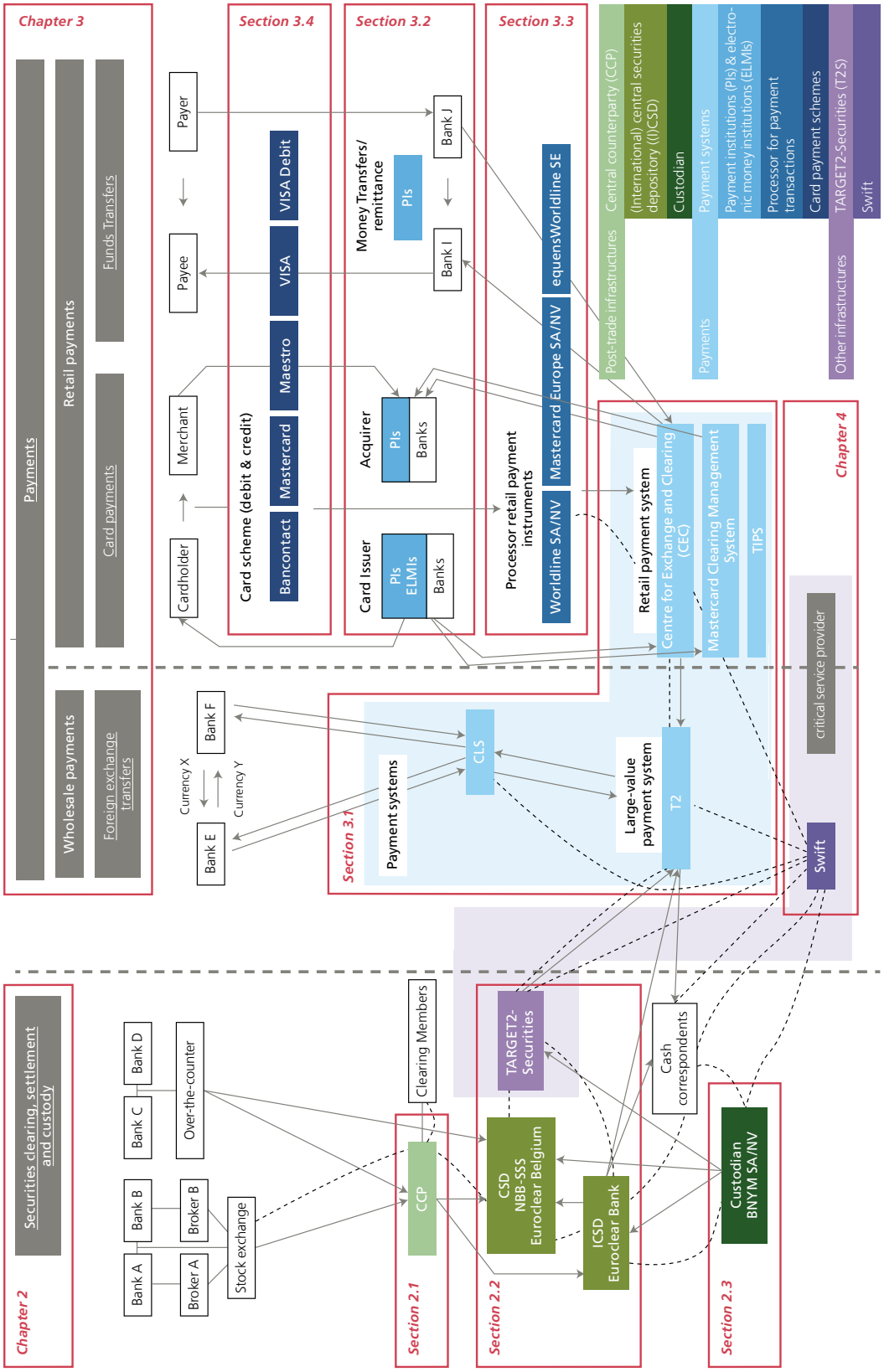
CLS, a settlement system for foreign exchange (FX) transactions is linked to the LVPS systems operated by central banks of 18 currencies (including T2 for EUR), making it possible to settle both legs of the FX transaction at the same time. CLS eliminates FX settlement risk when – due to time zone differences – 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 messaging service provider Swift is neither a payment system nor a settlement system, a large number of systemically important systems depend on it for their daily financial messaging. It is therefore considered as a critical service provider.

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, ranging from the object of the function, the authority responsible, the topics covered, and the regulatory framework and tools used. However, both oversight and prudential supervision activities, and the framework they rely 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 must 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[1] and focuses on systems established in or relevant for Belgium. Although Swift is not a payment, clearing or settlement infrastructure, many such systems use it, effectively making it 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 the prudential supervisory authority for individual financial institutions, as well as custodians and Payments Service Providers. 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 the national competent authority.

Some FMIs are subject to both oversight and prudential bank supervision, typically if the FMI operator has bank status (as is the case for Euroclear Bank). Worldline SA/NV is also subject to both prudential supervision (as a payment institution) and oversight (as a retail payment instruments processor). In such situations, the oversight activity and prudential supervision complement one another: 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 on which oversight focuses concern 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 a participant's insolvency (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 trigger contagion risks in financial markets. Prudential supervision seeks to ensure that institutions are financially robust at micro-prudential level, thus helping to maintain the trust of the institution's counterparties and thereby

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

promoting financial stability. Some types of risks are monitored by 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 tends to be based on maturity transformation (short-term deposits, long-term assets). The regulatory approach for credit, liquidity and operational risk for FMIs therefore differs from that for banks.

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 adhere 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 European Central Bank (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 synergies and align approaches between the oversight function and that of prudential supervision of 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 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, T2, T2S 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 the 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 which 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 2023)

	International cooperation		The Bank acts as the sole authority
	The Bank acts as lead authority	The Bank participates in the supervision, 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 depositories (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 processors Worldline SA/NV
Oversight	Critical service providers Swift	Other infrastructure TARGET2-Securities (T2S) [1]	CSD NBB-SSS
	Payment systems Mastercard Clearing Management System [2]	Payment systems T2 [1] CLS	
	Card payment schemes Mastercard Europe [2] Maestro [2]		Card payment schemes Bancontact [1]
			Payment processors [3] Mastercard Europe equensWorldline Worldline SA/NV Worldline Switzerland ltd
			Payment systems 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).

3 Only for certain Belgian activities – Act of 24 March 2017 on the oversight of payment processors.

BOX 1

Evolutions in the financial sector cyber threat landscape

The European financial sector has always been a target of choice for cyber threat actors. While their motivations remain the same (financial gain, information theft and service disruption), the last two years have shown notable evolutions in the associated threat actors and the way they operate. This article seeks to highlight specific developments that should be part of risk management activities of entities in our sector.

The rise of ransomware

Over the last few years, financially motivated threat actors have widely adopted ransomware and double or triple extortion attempts. In this modus operandi, the ransomware victim is first requested to pay to obtain the decryption key to recover the encrypted data. If negotiations fail, the threat actor requests a payment from the victim (double extortion) and/or pressures third parties involved (triple extortion) to avoid selling or making sensitive data public. The adoption of this modus operandi by several cyber-criminal groups and its profitability led to notable evolutions such as (i) the wider development of modular multi-stage malwares (comprising a first stage infection with the capability to download and execute more specific ones later), (ii) the leverage of cloud-based attack infrastructure (for phishing, malware delivery and command-and-control communication), (iii) the introduction of the ransomware-as-a-service model and (iv) the proliferation of initial access brokers (threat actors reselling a victim's network access to other actors).

While ransomware activity continues unabated, regardless of the geopolitical situation, it is crucial for the sector to adopt a defence-in-depth strategy including among other efficient backup, data loss/leak prevention, network segmentation, granular access management or threat hunting strategies. It is also worth noting potential changes in legal frameworks and cyber insurance policies which might evolve into forbidding ransom payments or no longer insuring losses due to ransomware attacks. Although these initiatives may lead to a reduction in the number of ransomware campaigns, it could also lead to ransomware incidents being kept quiet instead of reported.

Targeting the perimeter and beyond

Attack surface management has become increasingly complex nowadays for financial institutions, given threat actors not only exploit externally facing infrastructure but also the supply chain and third parties of these institutions. Targeting widely used technologies or third parties to get access to as many victims as possible becomes a more frequently used attack strategy.

On the one hand, mass exploitation of impactful zero- and N-days vulnerabilities (thus only recently known and potentially not patched yet) occurred widely in internet facing software such as mail servers or remote working solutions, as both are increasingly deployed since the pandemic. The exploitation of commonly used software and libraries highlights a concentration risk which must be kept under control via robust enterprise asset management, vulnerability management, patch management and secure development lifecycles.

On the other hand, advanced actors have increasingly been observed targeting the supply chain to infiltrate target companies. These attacks can take many forms, where notable cases range from the compromise of remote access technologies (e.g. SolarWinds), managed service providers (e.g. Okta) or the exploitation/backdooring of commonly used third party libraries integrated in a victim's software development lifecycle (e.g. Log4J vulnerabilities or backdoored Python packages). Addressing these attack vectors can be extremely challenging but can however be supported by a solid third-party risk management process and a secure software development lifecycle, as well as the "assumed breach" principle.

Payment chain manipulation and cryptocurrency attacks

Over the last two years, a significant decrease has been observed in successful campaigns manipulating the traditional payment chain of financial institutions (e.g., Central Bank of Bangladesh case in 2016). This is likely a consequence of the increased difficulty for threat actors to compromise such critical economic function since the establishment of customer security programmes such as the Swift CSP.

Threat actors known for targeting the traditional payment chain have since been shifting to attacking cryptocurrency assets. While this trend is currently still ongoing, recent regulatory initiatives (e.g., Market in Crypto-Assets) or cryptocurrency mining bans (e.g. Microsoft Azure bans) may turn this type of attack more difficult or less profitable. The financial sector might in such a scenario expect a resurgence of payment chain manipulations or an increase in Business Email Compromise (BEC) attacks and malicious insider coercion attempts, or even a surge in Credit Card fraud.

Cyber impact of the geopolitical crisis

Several potential scenarios were envisioned by cyber security experts since the beginning of the war in Ukraine. This section highlights two of the many types of observed cyber events that the sector could expect again in the future.

The first type is distributed-denial-of-service (DDoS) attacks performed by hacktivists. These were first targeting entities located in the countries directly involved in the war but are now also targeting nations and institutions supporting those countries or those that have imposed sanctions. While these attacks are having no or only minimal impact on institutions with robust DDoS mitigations in place, they could cause disruption by abusing unprotected internet facing hosts, misconfigured protection mechanisms or exploiting internet facing application vulnerabilities. The current situation emphasises the importance of reviewing the controls in place against this type of attack.

The second type is the risk of the sector being directly or indirectly targeted by destructive malware. While a scenario where destructive malware would indirectly spread (spillover effect, like the NotPetya case in 2017) outside the direct targets is now being regarded as unlikely, there were notable disruptive campaigns in 2022 such as the Gamaredon threat actor targeting Ukrainian government entities with destructive WhisperGate malware, initially disguised as ransomware. This type of threat is particularly relevant for national critical infrastructures and government institutions but should also be considered by the financial sector should the geopolitical situation worsen.

Conclusion

The developments highlighted in this article show the adaptability and opportunistic nature of threat actors targeting the financial sector. The cyber threat landscape is rapidly evolving, and institutions are advised to continue their efforts in bolstering and assessing their cyber resilience against such threats. These are also objectives of the Digital Operational Resilience Act and the TIBER framework that are presented respectively in chapters 5 and 8 of this Report.

2. Securities clearing, settlement and custody

FMIs and financial institutions that provide securities clearing, settlement and custody services are part of the post-trade securities landscape. Systems that clear trades conducted on a stock exchange or concluded between counterparties on the OTC market, and 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 for CCPs (section 2.1), (I)SDs (section 2.2) and custodians (section 2.3).

The (I)CSDs established in Belgium vary in the scope of their 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, as the overseer, is also considered as the relevant authority in the CSDR. The NBB-SSS, which is subject to oversight only, holds and settles public sector debt including securities issued by the Belgian federal government and by regional or local governments, and private sector debt issued by corporates, credit institutions or other entities.

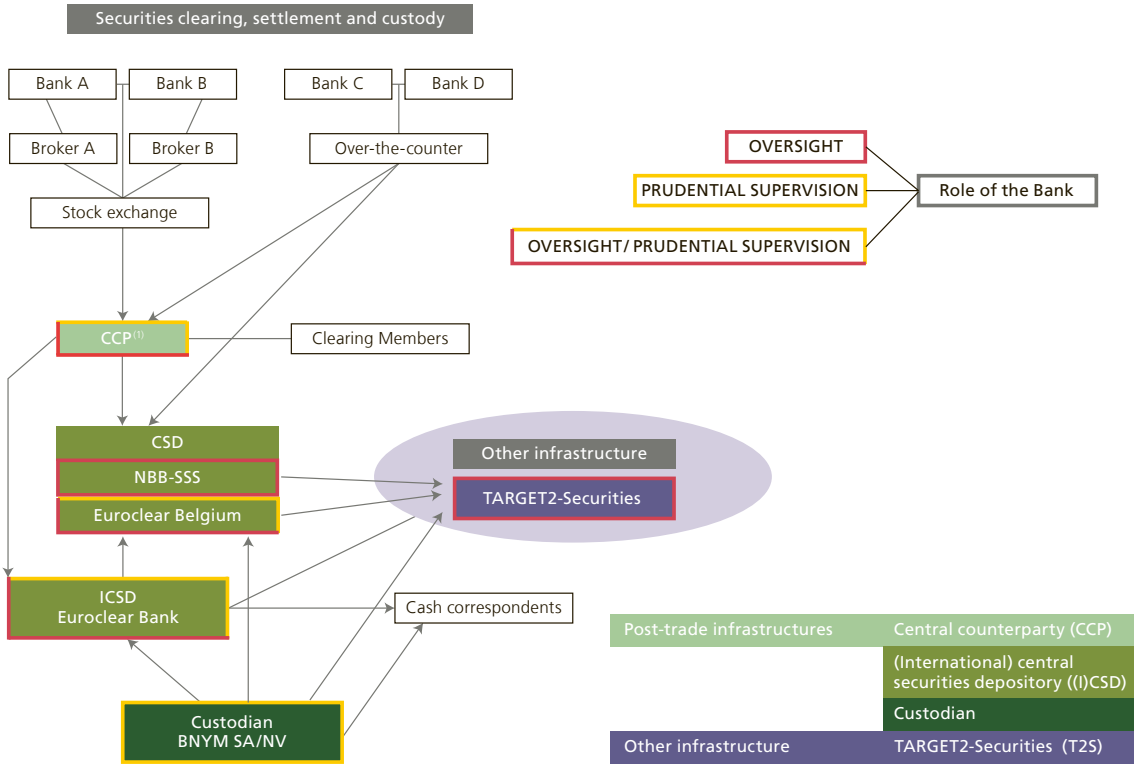
Daily settlement operations of Euroclear Belgium and NBB-SSS are outsourced to TARGET2-Securities (T2S), as in the case of other CSDs in Europe. T2S is not a CSD, but as it provides settlement services to many euro area and some non-euro area CSDs, it is essential that it enables participating CSDs to comply with the regulations applicable to them. The oversight of T2S is conducted by the Eurosystem. 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 monitor both the general organisation of T2S as a critical infrastructure (i.e. technical platform, legal basis, governance structure and comprehensive risk management framework), and the services it provides against an applicable subset of the PFMIs. The Bank participates in this cooperative arrangement.

BNYM SA/NV is a global custodian established in Belgium with links to multiple (I)CSDs allowing its clients to hold securities issued in markets worldwide. BNYM SA/NV provides custody services (i.e. providing securities safekeeping, settlement and investor services to their clients) and is supervised by the ECB under the framework of the SSM as a significant credit institution (SI).

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

Chart 2

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



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

2.1 CCPs

Changes in the regulatory framework

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

The framework that regulates CCPs, i.e. their resilience and recovery, and ultimately their resolution, was being further completed. The FSB, CPMI and IOSCO conducted further work on CCP financial resources. In March, they published a joint report CCP Financial resources for recovery and resolution[1]. The report informs on the use, composition and sufficiency of financial resources to cope with a CCP's recovery or resolution caused by participant default and non-participant default losses. It concluded on the need for further international work in this regard.

In August, CPMI and IOSCO published a discussion paper on CCP practices to address potential losses arising from non-participant default events and their management via recovery or orderly wind-down tools[2].

1 Available at https://www.bis.org/publ/othp46.htm.
2 Available at https://www.bis.org/cpmi/publ/d208.htm.

In September, BCBS-CPMI-IOSCO published their review of margining practices during the March 2020 market turmoil[1]. The analysis confirmed the substantive increase in variation and initial margin calls and identified areas for further policy work on the transparency, predictability and participant practices of margin calls. The relevance of this work was once again evident with the price surges in Europe for cleared energy contracts due to Russia's invasion of Ukraine[2].

Also in September, CPMI and IOSCO published a final paper on client clearing[3]. It describes the benefits and potential risks of new models that enable clearing members' clients to directly access CCP services and the effective porting – i.e. the transfer of the client's positions and assets in the event of default of its clearing member to a back-up member – and urges the industry to do further work in this respect.

In December, the European Commission (EC) tabled a proposal[4] including measures to make EU clearing more attractive and resilient by reducing excessive exposures of EU market participants to third-country CCPs that clear derivatives identified as substantially systemic for the EU's financial stability.

The EU Regulation on CCP recovery and resolution (CCP-RR) that sets out a framework for the recovery of a CCP, and the rules to ensure in resolution the continuity of a CCP's critical function was being further implemented. In May, ESMA published final reports[5] containing draft implementation legislation related to resolution colleges, CCP financial resources in resolution, safeguards for clients and CCP resolution plans. In November, the Commission published its implementing Regulation[6] that sets out the methods for calculating the so-called "second skin", i.e. a second layer of the CCP's contribution in recovery.

Prudential and oversight approach

In July, ESMA published the outcome of its fourth supervisory stress test for CCPs[7] covering EU CCPs as well as third-country CCPs that are systemically important to the EU, focusing on counterparty credit, concentration and operational risk. The results confirm the overall resilience of CCPs, while identifying areas for improvement for some CCPs in relation to concentration and operational risks.

As required under EU legislation, the National Bank of Belgium takes part in five EU CCP supervisory colleges[8] that are relevant for the Belgian markets, participants or CSDs. Post-Brexit, the Bank also takes part in the UK CCP colleges of LCH Ltd and ICE Clear Europe Ltd, even though they are no longer EMIR supervisory colleges.

Priorities for the ongoing supervision of EU CCPs are set by the national competent authorities, taking into account the college members' requests. New CCP services or products, significant risk model changes and recovery plans are approved by the CCP's national competent authority, taking into account its supervisory college's opinion. The recovery plans of most EU CCPs that stipulate how to allocate default and non-default losses to shareholders, clearing members and clients, were initially assessed under the applicable CCP-RR regime.

National EU CCP resolution authorities continue to plan for CCP resolution occurrences and establish the resolution colleges required by CCP-RR. To date, the Bank is involved in four EU CCP resolution colleges that were set up under the CCP-RR[9].

1 Available at https://www.bis.org/press/p220929.htm.
2 See, for example, the ECB Banking Supervision newsletter of November 2022, available at https://www.bankingsupervision.europa.eu/press/publications/newsletter/2022/html/ssm.nl221117.en.html.
3 Available at https://www.bis.org/cpmi/publ/d210.htm.
4 Available at https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7348.
5 Available at https://www.esma.europa.eu/press-news/esma-news/esma-publishes-final-reports-ccp-resolution-regime.
6 Available at https://ec.europa.eu/transparency/documents-register/detail?ref=C(2022)8434&lang=en.
7 Available at https://www.esma.europa.eu/sites/default/files/library/esma91-372-2060_4th_esma_ccp_stress_test_report.pdf.
8 This refers to the CCP supervisory colleges of LCH.SA (FR); Eurex Clearing AG (DE), EuroCCP (NL), CC&G, now EuronextClearing (IT) and Keler CCP (HU).
9 The CCP resolution colleges of LCH SA (FR); ECAG (DE); Cboe (NL) and Keler CCP (HU).

BOX 2

Securities trading, clearing and settlement in Europe – Belgian FMIs

Under its Capital Markets Union plan, the European Commission seeks as a long-term strategy to build integrated EU capital markets. Financial market infrastructure at trade and post-trade level constitute the backbone to process capital markets transactions, a quality that is underpinned by legal requirements to use the FMI under certain conditions[1]. Besides regulation, economics drive the trade and post-trade services. Economies of scale, i.e. decreasing average production costs in relation to the total volumes produced, and economies of scope, i.e. positive network externalities whereby the user of the service derives more value as more users use the same network service, apply when providing market infrastructure services. Also, the seamless conclusion of a trade and its clearing and settlement is important. Thus, exchanges do have an interest in the well-functioning of post-trade services.

Compared to other countries such as the United States, the European trade and post-trade environment remains considerably fragmented leading to efficiency loss and increased operational risk. Today, in the EU-27, there are 27 (national) stock exchanges[2], 11 CCPs[3] and 29 CSDs[4]. The below graph shows a selection of the corporate groups owning the biggest FMIs involved in the trading, clearing and settlement of the European cash markets. The biggest EU-27 cash markets belong to the Euronext, Deutsche Börse or Nasdaq group. All three market groups have an own CCP while the biggest CCP for fixed income is currently LCH SA in France that is part of the London Stock Exchange Group. At settlement level, big EU CSDs also belong to Euronext and Deutsche Börse, and to the Euroclear group that is only active in CSD/settlement services.

Horizontal integration of EU FMIs is progressing slowly and in different ways. Full corporate mergers of same-level FMIs remain scarce. For instance, there was one at CCP level in 2000 when the Euronext markets started using the French LCH SA as their single CCP for their Amsterdam, Brussels, Paris and Lisbon markets. Horizontal integration can also occur operationally or contractually while maintaining separate legal entities, e.g. by using a common platform and a common contractual framework. Examples include the Euronext markets at trading level and the ESES CSDs, comprising the CSDs Euronext Belgium, Euronext France and Euronext Netherlands at settlement level. Also, on a broader scale and across corporate groups, the ECB's T2S platform has integrated and harmonised almost all euro area CSD settlement services without reducing the number of CSDs. Finally, CCPs are integrating their services horizontally by establishing interoperability links between themselves such as the link between LCH SA and Euronext Clearing (previously the Italian CC&G) for fixed income, for example. And CSDs that are linked as an investor CSD to an issuer CSD are doing the same.

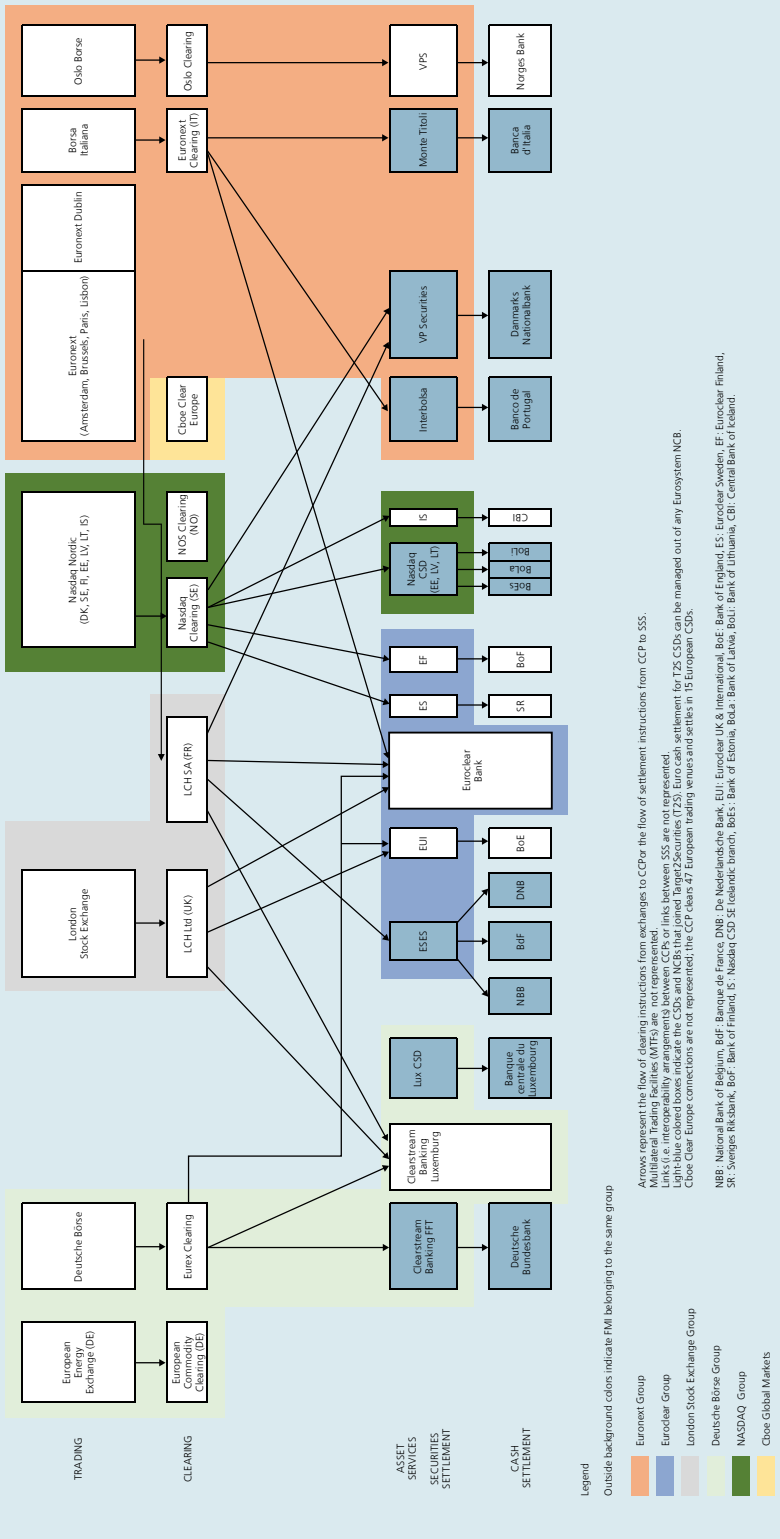
1 Requirements to use a trading venue when issuing securities against public funding, and Art. 23 of MiFIRII introduces a share trading obligation requiring EU investment firms to trade shares on a trading venue or with a systemic internaliser. The obligation to record the securities issuance in a CSD is stipulated in art. 3 of CSDR. Other than for derivatives there is no requirement to clear cash market securities trades in a CCP.

2 The EU trading activities are overall more fragmented and diverse. According to ESMA, in 2020, there were 127 regulated markets (RMs), 142 multilateral trading facilities (MTFs), 27 organised trading facilities (OTFs) and 172 systemic internalisers (SIs) in the EU.

3 ESMA – List of Central Counterparties authorised to offer services and activities in the EU.

4 ESMA70-155-11635 – CSD Register.

European financial market infrastructure – Biggest firms offering exchange trading, clearing and settlement for the cash markets



Many FMIs in the EU are now part of an exchange group that vertically integrates the value chain, and thus offer the full service package across the value chain via in-group FMIs. The Euroclear group CSDs – that settle Euronext or Nasdaq market trades – are an exception in this regard.

Within the logic of the value chain linking trading, clearing and settlement, most exchanges have built an integrated trade and post-trade solution. Even so, these integrated services are not provided on an exclusive basis. European Union legislation[1] gives exchanges, CCPs and CSDs the right of mutual access throughout the (vertical) value chain of trading-clearing-settlement, implying they can choose their place of clearing or settlement, or – vice-versa – acquire a trade feed or a CCP feed for processing the trade in the CCP or CSD.

Netherlands-based Euronext NV, whose main business activity is trading, operates the Euronext markets, including Euronext Brussels. In 2021, Euronext NV acquired the Borsa Italiana group comprising the Italian stock exchange, the CCP Euronext Clearing and the domestic CSD Monte Titoli. This will impact the clearing of Euronext trades and potentially their settlement.

The French CCP LCH SA now clears most of the Euronext markets, but Euronext intends to directly manage the clearing of its own markets. It announced in November 2021 that Euronext Clearing will be the CCP of choice for its cash and derivatives markets although it will continue to offer an open access CCP model for cash equity clearing, in particular with LCH SA. Under the envisaged preferred clearing model, both LCH SA and the Amsterdam-based Cboe (previously EuroCCP and now belonging to Cboe Global Markets) can (continue to) connect to the trade feeds of the Euronext cash markets but will only be able to deliver the clearing service where both parties of the trade clear in the (same) CCP.

At settlement level, Euronext group also owns a number of CSDs (besides Monte Titoli (Italy), there is Euronext VPS (Norway), Interbolsa (Portugal) and VP Securities (Denmark)), but the bulk of its cash markets are still settled by Euroclear group CSDs. Securities that have already been issued in a Euroclear group CSD will likely remain there considering the costs of switching to another CSD. New securities could be issued directly in the Euronext CSDs if issuers value the full vertical service offering of the Euronext group.

1 Dedicated FMI access requirements to that end are stipulated in Articles 35 and 36 of MIFIR, Articles 7 and 8 of EMIR and Article 53 of CSDR.

2.2 (I)CSDs

Changes in the regulatory framework

In February 2022, the settlement discipline regime (SDR) entered into force. As part of CSDR, this regime aims to improve settlement efficiency, the rate at which securities transactions settle on the intended settlement date, in the European Economic Area. It ushered in several measures to encourage market participants to settle transactions on the intended settlement date. More information regarding the SDR can be found in box 3.

On 2 June 2022, the Regulation on a pilot regime for market infrastructures based on distributed ledger technology (DLT) was published[1] in the Official Journal of the European Union. The regime creates a new EU status for market infrastructures based on DLT in a context of conditional and regulated experimentation. It aims to identify regulatory obstacles to DLT and may eventually lead to a more permanent and adapted regulatory regime for trading and post-trading services. The DLT pilot regime has applied from 23 March 2023.

The review of the CSD Regulation (CSDR) has also been ongoing in 2022 and 2023 focusing on such things as relevant aspects of the supervisory process (e.g. frequency of CSDR review and evaluation, cooperation between authorities) and a mandatory buy-in regime for settlement fails.

1 Regulation (EU) 2022/858 of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology, and amending Regulations (EU) No. 600/2014 and (EU) No. 909/2014 and Directive 2014/65/EU.

BOX 3

Implementation of the Settlement Discipline Regime

On 1 February 2022, the settlement discipline regime (SDR) under the CSD Regulation (CSDR) entered into force. The overall aim of the settlement discipline regime is to enhance settlement efficiency, i.e. the rate at which securities transactions settle on the intended settlement date, in the European Economic Area.

While the CSD Regulation dates from 2014, the Regulatory Technical Standards (RTS) on settlement discipline were only supposed to enter into force on 13 September 2020. However, this was initially postponed to 1 February 2021[1] to allow time to establish some essential features for the functioning of the new framework by (I)CSDs and market participants in general, including the development of a common T2S penalty mechanism for T2S CSDs. During the COVID-19 crisis, stakeholders asked for a further postponement of the entry into force of the RTS due to the impact of the pandemic on the overall implementation of regulatory projects and IT deliveries by CSDs and their participants, as well as the higher probability of not reaching compliance by 1 February 2021. Following the Commission's tabling of an ESMA proposal with regard to a new implementation timeline and subsequent non-objection by the Parliament and Council, the new date for entry into application of these rules was set as 1 February 2022.

The settlement discipline regime aims to encourage market participants to avoid settlement fails. It encompasses a set of common requirements for CSDs and their participants to comply with. Its two main elements are the measures to prevent settlement fails and measures to address those fails.

Regarding the prevention of settlement fails, CSDs are required to have different measures and procedures to facilitate the settling of instructions on the intended settlement date. Those measures range from ensuring the settlement process is automated, allowing for the partial settlement of instructions, to CSDs' participants' access to information on their transactions. Supervisors need to check whether the CSDs

1 ESMA70-151-2895 – CSDR RTS on Settlement Discipline – postponed entry into force.

have made the required facilities available to their participants to facilitate the timely settlement of transactions with the aim of improving their settlement efficiency rates.

The measures to address settlement fails revolve around three aspects: (I) the reporting of settlement fails by the CSDs to the authorities, (II) the application of cash penalties for transactions that fail to settlement in a timely manner, and (III) the buy-in regime, which aims to enforce non-settled transactions.

Regarding the reporting of settlement fails, CSDs are required to monitor the settlement efficiency rate of their participants, report to the competent and relevant authorities and disclose data on settlement efficiency. Supervisors have to make sure that CSDs are able to collect the required data in a correct and timely manner.

The requirement for the application of cash penalties is a key aspect of the settlement regime. CSDs are obliged to calculate and apply a cash penalty – a financial sanction – for transactions that have failed to settle on the intended settlement date. Moreover, CSDs have to be able to collect the penalties from failing delivering participants and redistribute them to the receiving CSD participants. Therefore, supervisors need to analyse whether CSDs have the technical capability to calculate and process these settlement fails penalties.

These two measures to address settlement fails effectively entered into force on 1 February 2022. The third measure – application of the mandatory buy-in regime – has been postponed as it may increase liquidity pressure and the costs of securities at risk of being bought in [1]. This postponement should provide some time in which to reassess the effects of a mandatory buy-in regime as part of the broader revision of the CSDR (CSDR Refit) that is currently ongoing. Depending on the outcome of this assessment, the rules on mandatory buy-ins could still be amended.

1 Commission Delegated Regulation (EU) 2022/1930 of 6 July 2022 amending the regulatory technical standards laid down in Delegated Regulation (EU) 2018/1229 as regards the date of application of the provisions related to the buy-in regime.

Prudential and oversight approach

The CSDR, implementing the CPMI-IOSCO Principles for CSDs in Europe, requires the Bank, as the national competent authority under the CSDR, to conduct an annual review and evaluation (under CSDR Art. 22) of Euroclear Bank and Euroclear Belgium. At the beginning of the review and evaluation process, the Bank consults other authorities as required ("relevant authorities" as defined in the CSDR), the FSMA and the competent authorities from the countries where the Euroclear group has a CSD). For Euroclear Belgium, the assessment is coordinated with those conducted by the French and Dutch competent authorities for Euroclear France and Euroclear Nederland respectively, as the operations, governance and rulebooks of the three CSDs – together the ESES CSDs – are aligned to a large extent. For Euroclear Bank, the final outcome of the review and evaluation was shared with the competent authorities of the countries for which the ICSD is substantially important, as well as with EBA and ESMA (see box 4).

As Euroclear Bank is also subject to banking regulation, the NBB conducts next to the CSDR review and evaluation also a yearly Supervisory Review and Evaluation Process (SREP) for banks. The Bank is synergising all

assessment frameworks applicable to Euroclear Bank, meaning CSDR and PFMI principles and key considerations are taken onboard into the banking-regulation-defined SREP analysis.

Following the UK's withdrawal from the European Union, in order to continue to provide CSD services in the UK, Euroclear Bank must be recognized by the Bank of England. As required by article 25 of the UK CSDR[1], a cooperative arrangement between the Bank of England and the non-UK CSD's authority, in casu the NBB, has to be established. A new Memorandum of Understanding with the Bank of England was signed in January 2023, renewing the already existing cooperation arrangement.

The impact of Russian sanctions and countermeasures adopted by Russia on Euroclear Bank remained an important attention point for the Bank in its supervisory activities. Blocked securities positions due to sanctions still generate income and redemption payments impacting the size of Euroclear Bank's balance sheet significantly. On the other hand, Russian countermeasures affect holdings of Euroclear Bank on behalf of its participants with a Russian nexus.

Euroclear Bank intends to join TARGET2-Securities (T2S) as a participating (I)CSD. By connecting to the T2S platform, Euroclear Bank clients will have the choice between euro settlement in commercial bank money and euro settlement in central bank money. The project has the potential to optimise their liquidity management and reduce financing costs. It will be implemented in phases. The mobilisation of collateral for monetary policy operations of National Central Banks (NCBs) will be the first use case. It was rescheduled from November 2023 to April 2024 after the Eurosystem delayed its consolidation of TARGET2 and T2S to 20 March 2023. The Bank is monitoring this Euroclear Bank project and analysing potential risks that could be linked to its implementation.

1 Regulation (EU) No. 909/2014 of the European Parliament and of the Council of 23 July 2014, as amended and retained in UK law.

BOX 4

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.

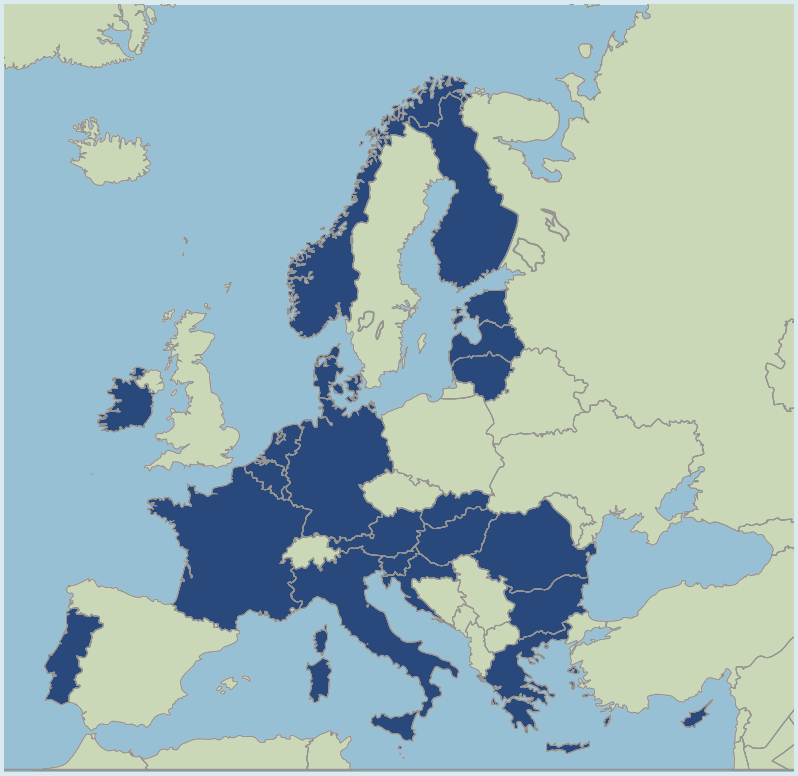
Under the CSDR, the Bank, as the competent authority, also needs to involve other authorities in the supervision of (I)CSDs established in Belgium. The CSDR identifies as "relevant authorities" the authorities responsible for oversight, central banks in the EU in whose books cash is settled, and central 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 a 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 also considered a relevant authority. The Eurosystem is likewise a relevant authority for Euroclear Bank, which settles in euro too. In 2021, the Danish and Norwegian central bank have become relevant authorities as well for Euroclear Bank since, in accordance with the ESMA methodology, their currencies were considered a relevant currency for Euroclear Bank until ESMA's next yearly calibration.

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)	MoU on cooperation and exchange of information with regard to the relationship of Euroclear SA with the (I)CSDs of the Euroclear group; Euroclear SA being both the parent holding company and service provider to the Euroclear group entities
Euroclear Bank	
Central banks of issue of major currencies in Euroclear Bank (Federal Reserve System, BoE, BoJ, Reserve Bank of Australia and ECB as observer).	Multilateral oversight cooperation with the relevant central banks of issue of the major currencies settled in Euroclear Bank
ECB	Bilateral oversight cooperation on specific aspects of Euroclear Bank relevant for euro area financial stability
Bank of England	Following the UK's withdrawal from the European Union, in order to provide CSD services in the UK, Euroclear Bank must be recognized by the Bank of England. As required by the UK CSDR, a cooperative arrangement between the Bank of England and the NBB has to be established
Bank of Japan	Bilateral oversight cooperation on specific aspects of Euroclear Bank relevant for Bank of Japan
Central Bank of Ireland	Bilateral cooperation with regard to the settlement of Irish bonds, some exchange-traded funds (ETFs) (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 prudential supervision of the ICSDs Euroclear Bank and Clearstream Banking SA (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 addition to the FSMA and the relevant authorities, the competent authorities from EEA countries where Euroclear group has a CSD are involved in the annual review and evaluation process of Euroclear Belgium and Euroclear Bank. As Euroclear Bank is of substantial importance for many EEA countries, the NBB shares an outcome report with authorities in those countries.

EEA Countries for which Euroclear Bank is of substantial importance



1 Austria, Belgium, Bulgaria, Croatia, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, The Netherlands, Norway, Portugal, Romania, Slovakia and Slovenia.

As mentioned above, the settlement discipline regime (SDR) provisions of the CSDR entered into force in February 2022. The Bank has monitored the CSDs' compliance with these provisions, including the required statistical reporting on settlement fails (i.e. transactions that are not settled on the intended settlement date).

Because cyber threats are continuously evolving, cyber security continues to be a top priority for the Euroclear group. Multi-year projects are ongoing to further strengthen cyber capabilities. Continuous investment is key to being equipped with the latest products and to benefit from the most advanced technologies. However, it should be stressed that the cyber domain is far broader than only technical measures, i.e. this is the reason why training and testing of the system's users is critical. Currently, many attacks use the technic of "(spear)phishing", where targeted users have an incentive to click on links, thereby enabling the installation of malware. Recruitment is also an important point: as cyber is growing in importance, more job opportunities are becoming available, complicating the recruitment (and retaining) of cyber specialists. Finally, senior management's commitment remains key to success. All these projects are being closely followed up and discussed with other authorities of the Euroclear group entities.

In January 2023, the Euroclear Bank participants' security controls framework entered into force. The framework requires participants to adhere to certain controls and good practices to appropriately secure their on-premises IT environments connecting to the Euroclear system. By requiring the compliance of participants with mandatory

security controls, Euroclear Bank aims to improve its cyber security capabilities and to follow regulatory expectations.

In the context of the group's "digital & innovation" strategy, Euroclear Bank has continued working on a "digital FMI" (DFMI) project. It allows for the possibility to issue and store on a dedicated component of its SSS securities using distributed ledgers. In a first phase, it is focussing on the primary market issuance as secondary market settlement is processed on the legacy platform. The technical launch of the project occurred end of April 2023, the required updates of the Euroclear Bank contractual documentation were published in May 2023. As a next step, Euroclear Bank will accept the first issuances of digitally native notes in pilot format with a small number of participants and issuers, and for a limited number of medium-term bonds.

ESG (Environment Social Governance) is one of the pillars of the Euroclear group's strategy. A 2021 paper[1] released jointly with PwC outlines opportunities for FMIs to support market participants and asset classes, including (i) encouraging greater sustainable finance issuance, through reducing infrastructure, regulatory and informational barriers to issuance, (ii) processing ESG information flows including ESG metrics, disclosure and assurance, and (iii) expanding the market to more asset classes and participants.

In that context, in January 2022, the Euroclear group made an investment in Greenomy, a Belgian sustainable finance technology start-up that has as objective to help companies, banks and asset managers to comply with new EU sustainable finance legislation. A prerequisite to promoting sustainable finance is the identification of securities as "sustainable" or "green" and Greenomy's platform will capture key data about ESG bonds accepted in one or more CSDs of the Euroclear group. Such data enables computation of a financial product's sustainability rating under the EU Taxonomy Regulation.

At the end of 2022, Euroclear SA also decided to acquire Goji[2], a London-based provider of digital access to private funds, further developing its funds strategy, following the acquisition of the MFEX funds distribution platform earlier on. Aside from such acquisitions, other developments led to changes in the governance structure of the Euroclear group. In early January 2023, Euroclear Investments, the group's financial investment holding company and its long-term bond issuer, moved its headquarters from Luxembourg to Belgium, after approval by the National Bank of Belgium. Also in January 2023, Euroclear SA formally filed for non-objection by the Bank to plans to set up a branch in Krakow, Poland. The objective for Euroclear SA is to gain access to additional talent pools to enable the recruitment of various profiles. The Bank declared (its) non-objection in March 2023.

In 2022, the NBB-SSS was selected as issuer CSD and settlement agent for the EU Issuance Service (EIS)[3]. Through the EIS, the NBB-SSS will issue debt securities to fund strategic plans like the NextGenerationEU (NGEU) recovery plan[4]. This recovery package will be funded by resources made available by the issuance of debt securities, which are expected to reach a value of € 800 billion by 2026. On 12 July 2022, the Letter of Intent that underpins the EIS was signed by the NBB, the European Commission and the European Central Bank.

Although CSDs operated by members of the ESCB are exempt from the authorisation and supervision requirements of the CSDR[5], some of its prudential requirements do apply to them. Under the new regime for granting eligibility to securities settlement systems and links for their use in Eurosystem credit operations, on the basis of the CSD's compliance with the CSDR requirements, and in cooperation with the Eurosystem, the

1 Available at https://www.euroclear.com/newsandinsights/en/Format/Whitepapers-Reports/sustainable-finance-market.html.

2 Subject to regulatory approvals.

3 The EU issuance service is a project via which the settlement of all bonds issued by the European Commission on behalf of the EU will be processed through the Eurosystem's payment and settlement infrastructure. Once the EU issuance service is in place, a Eurosystem central bank – in this case, the National Bank of Belgium – will serve as issuer CSD and act as an agent for settlement services, while the European Central Bank will act as paying agent for all EU debt securities.

4 NextGenerationEU is the EU's temporary recovery instrument to support the economic recovery from the coronavirus pandemic and build a greener, more digital and more resilient future.

5 Under Article 1(4) of the CSDR.

NBB exercises its overseer role by conducting a yearly review and evaluation of the NBB-SSS against the CSDR requirements which are relevant from a "user perspective" [1].

With regard to operational risks, and relevant for all (I)CSDs subject to its supervision and oversight, the Bank is focusing this year on operational resilience and third-party outsourcing arrangements, including policies and practices regarding cloud service providers.

1 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 effectively a user of the NBB-SSS, it needs assurance that the NBB-SSS is safe to use.

BOX 5

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 2022, Euroclear Bank had more than 1 800 participants. Its participant base consists mainly of non-domestic entities, including almost 100 central banks, more than 40 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 SA (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 notaries 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.

To provide services in international bonds and a wide range of foreign securities, 100 different currencies are eligible in the system operated by Euroclear Bank. Securities can be settled against payment in a Euroclear settlement currency [1] (46 currencies) which may differ from the denomination currency [2].

At the end of 2022, the value of securities deposits held on Euroclear Bank's books on behalf of its participants amounted to € 17.5 trillion equivalent (up from € 17.1 trillion in 2021). After EUR (50 %), USD is the main denomination currency (28 %), followed by GBP (10 %). 51 % of securities deposits are in international bonds, for which issuers can choose the denomination currency and the governing law for their securities.

Regarding settlement turnover, the number of transactions settled in Euroclear Bank in 2022 came to 163.3 million (up from 146.9 million in 2021). In value terms, this represents € 692.2 trillion (up from € 652.6 trillion in 2021). 67 % of settlement turnover, free-of-payment and against-payment transactions,

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.

was denominated in EUR, after USD (15 %) and GBP (9 %). In terms of settlement turnover per security type, compared to securities deposits, international debt accounts for 19 % while the bulk is composed of other types of securities such as domestic debt and, to a lesser extent, equities or exchange-traded funds.

The interconnectivity of Euroclear Bank with other FMIs is a critical component in the Euroclear group strategy to establish a common pool of collateral assets in which Euroclear group entities provide collateral management services as a triparty agent taking over the collateral management tasks (including collateral selection, valuation and substitution) from its participants during the lifecycle of the transaction concluded between two participants. At the end of 2022, at group level, the average daily value of triparty collateral managed by the Euroclear (I)CSDs reached € 1.8 trillion equivalent.

Composition of securities deposits and turnover in percentage, end of year 2022

Source : Euroclear.

2.3 Custodians

Changes in the regulatory framework

In 2022, the regulatory framework applicable to custodians remained unchanged.

Supervisory work in 2021 and priorities for 2022

BNYM SA/NV is considered as a significant institution, which implies that BNYM SA/NV falls under the direct supervision of the SSM. The supervisory work relating to the CRD/CRR regulatory framework is therefore carried out jointly by the Bank and the ECB within the SSM. BNYM SA/NV is also subject to monitoring by the Bank as regards the specific requirements applicable to depository banks and client asset protection rules.

BNYM SA/NV is a subsidiary of BNY Mellon, a US-based global systemic bank. At the end of 2022, BNYM SA/NV had one subsidiary and several branches in Europe through which it operates in the local markets. BNYM SA/NV has branches in Luxembourg, Frankfurt, Amsterdam, London, Paris, Dublin, Milan, Madrid and Copenhagen. The ECB and NBB also granted permission to BNYM SA/NV in 2022 to open an operational branch in Poland.

BNYM SA/NV is the group's custodian for European clients, and the European gateway to the euro area markets and payment infrastructures within the BNYM group. BNYM SA/NV settles transactions in a wide range of currencies, the main ones being EUR, GBP, USD and JPY (see box 6 on the international dimension). In this perspective, in 2022, the Joint Supervisory Team (JST) focused on the follow-up of the 2021 review of the management of intraday and short-term liquidity risk.

The Russia-Ukraine war also affects BNYM SA/NV. Given its specific business model, BNYM SA/NV had to correctly implement sanctions that were common to every bank and financial intermediary (albeit due to its global presence, BNYM SA/NV has to implement different sets of sanctions) but also specific attention points relating to activities like depository receipts (DRs) etc. The JST had regular interactions over 2022 with BNYM SA/NV and BNYM group to follow up on these topics.

In 2022, governance (due to the group's global organisation) and operational risk (due to the group's specific mix of activities) were the most important risk areas and will remain of high importance within the 2023 review cycle. Being a global custodian, BNYM group operates according to a "follow the sun" model which enables it to process clients' transactions and related services continuously around the globe across different time zones. This is mainly achieved by having established BNYM group entities worldwide, working on common platforms and multiple intra-group outsourcing arrangements. Such a model can bring efficiency and resiliency advantages (e.g. back-up locations), but it can also bring organisational complexities and additional attention points (such as the monitoring of outsourced activities). Legal entity independence, budget autonomy and supervision of outsourcing arrangements continue to be main areas of focus. Besides, a custodian plays a central role in the functioning of globalised financial markets. BNYM group and BNYM SA/NV are expected to build a highly resilient organisation (e.g. by ensuring sufficient and adequate fall-back capabilities between regional operational centres), not least to help maintain stability in the functioning of markets and to meet client expectations. Protection against and management of cyber risks and the continuous monitoring of firms' operational resilience was and still is part of the supervisory work. In the 2023 review cycle, attention is being paid to risk data aggregation and reporting, which is an important element in accurate monitoring of operations and measuring the size of the different risks (credit, market, liquidity, operational, etc.).

After years of negative or low interest rates, interest rates start to rise again. The level of market risk (including spread risk) and interest rate risk as well as the management of these risks and compliance with EMIR Regulation are areas of attention in the 2023 review cycle.

Last year, The Bank initiated an in-depth methodological analysis focused on the coverage and treatment of custody-related risks (like restitution risk) and the impact of business model-related specificities on other risk types (chapter 6 on restitution risk). The Bank will continue this work in 2023 by launching implementation of the analytical framework that was drawn up to measure these specific risks. Geopolitical tensions, like the Russia-Ukraine conflict, are clear evidence that restitution risk is growing. The introduction of digital assets will add another dimension to restitution risk due to their specific nature and related risks, which the Bank monitors closely.

Last but not least, the NBB will continue to devote increasing attention to climate risk (see chapter 7 on climate risk monitoring in financial market infrastructures, payment transactions processors and messaging services).

BOX 6

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

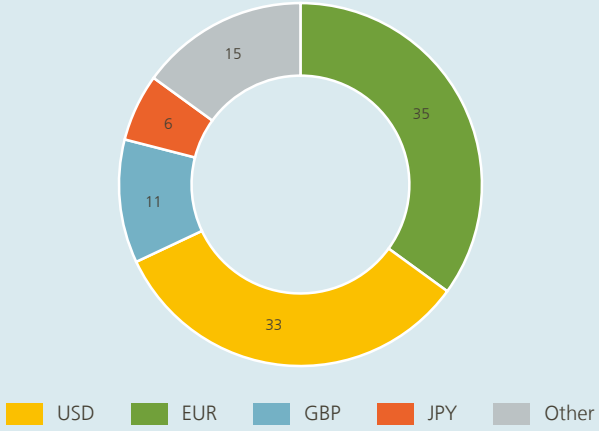
The Bank of New York Mellon, a banking group incorporated in the US, is the largest custody bank in the world in terms of assets under custody ($ 44 trillion as at December 2022, down by 6 % on the previous year). It is a global systemically important bank (G-SIB), providing asset and investment management 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, branches in Luxembourg, the Netherlands, Germany, France, Ireland, Italy, the UK, Denmark and Spain through which it operates in these local markets and an operations-only branch in Poland (with no access to the local market). BNYM SA/NV qualifies as other systemically important institution (O-SII) as assessed by the Bank based on the relevant EBA guidelines.

By the end of 2022, BNYM SA/NV served almost 4 000 international, institutional customers[1] on whose behalf it held € 2.8 trillion equivalent assets under custody, denominated in more than 80 different currencies[2]. The majority of these assets are denominated in EUR (35 %), followed by USD (33 %), JPY (11 %) and GBP (6 %). 50 % of these assets are bonds and 50 % of these assets are shares. In terms of settlement activity[3], BNYM SA/NV processed about 9.1 million transactions worth 52.3 trillion equivalent in 2022 ; the main currencies are USD (59 %), EUR (29 %), GBP (9 %) and DKK (1 %)[4].

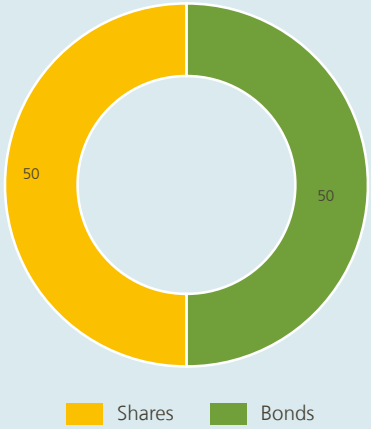
1 Compared to last year the number of clients is reported based on the holding view, providing more granularity. The number of clients, based on this definition steadily increased from 3 600 in 2020 to 3 800 last year and almost 4 000 this year.
2 Other important eligible currencies include DKK, CAD, CHF and AUD.
3 Value of BNYM settlement activity is based on receipt and delivery instructions.
4 Compared to last year, the scope of the data related to transactions has changed, this change also impacts the graph on Settlement Value by currency.

Composition of assets under custody and turnover in percentage, end of year 2022

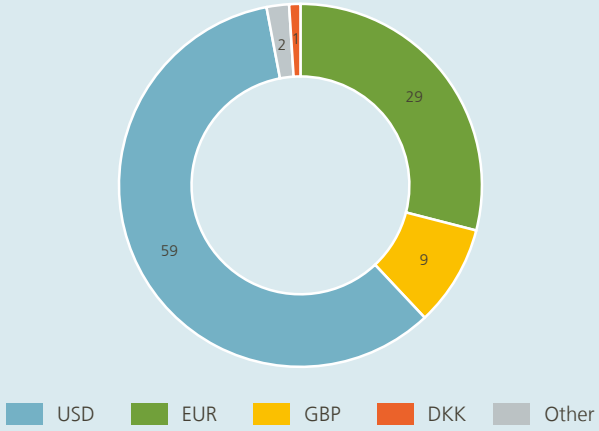
Assets under custody, per currency (%), end of year 2022



Assets under custody, per security type (%), end of year 2022



Settlement turnover value, per currency (%), 2022



1 Source: BNY Mellon.

3. Payments

The Bank has broad responsibility in the payments sphere 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 aims to ensure safe, stable and secure payment service providers delivering payment services to end users.

The interest of central banks in the payments sphere 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, and confidence in the currency, as well as contributing to a safe, reliable and competitive environment.

Section 3.1 covers the two payment systems at the heart of the Belgian payment infrastructure: T2[3] and the Centre for Exchange and Clearing (CEC). T2 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 T2, 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)[4]. This Regulation lays down the – mainly quantitative – criteria which, once exceeded, lead to the designation of the entity concerned 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 PSPs (mainly banks). This category of non-bank PSPs for retail payments provides respectively payment services and the issuing, redeeming and distributing of electronic money. ELMIs may also provide payment services and, given their ability to issue electronic money to the public, are subject to a stricter prudential regime, such as more stringent capital requirements.

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 As of 20 March 2023, the new payments system T2 went live and replaced TARGET2. For more detailed information, see https://www.ecb.europa.eu/press/pr/date/2023/html/ecb.pr230321~f5c7bddf6d.en.html.

4 Available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32020D0026(01)&from=EN.

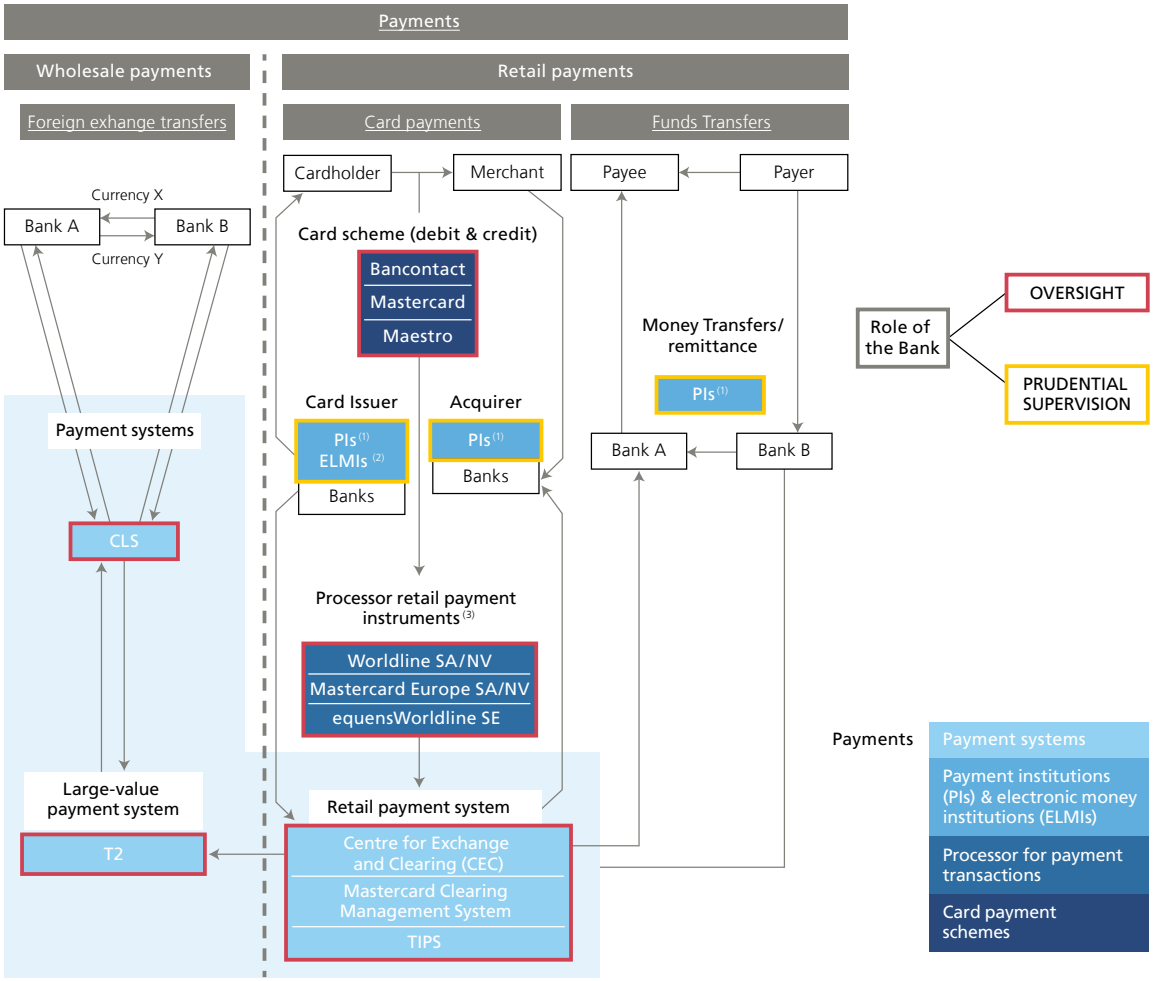
As an acquirer[1] and processor of retail payment instruments in Belgium, Worldline SA/NV is subject to both prudential supervision and oversight. The Bank's activities in that respect are covered in section 3.3.

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

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

Chart 3

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



1 Payment institutions (PIs).
2 Electronic money institutions (ELMIs).
3 Only the Belgian activities of equensWorldline SE are overseen by the NBB. Worldline Switzerland ltd is also designated as systemic processor for its switching activities for Bancontact according to the Law of 24/03/2017 regarding the oversight of payment processors and has specific obligations in that framework but it is not overseen by the NBB.

3.1 Payment systems

Changes in the regulatory framework

There were no changes to the Belgian and Eurosystem regulatory frameworks in 2022.

Oversight priorities / activities in 2022

Since May 2020, the Mastercard Clearing Management System (MCMS) operated by Mastercard Europe (MCE, established in Belgium) has been designated as a fifth Systemically Important Payment System (SIPS) with a pan-European reach, based on a number of mainly quantitative criteria, listed in the SIPS Regulation itself. As such, MCMS is subject to the joint lead oversight of the ECB and the NBB.

In the course of 2022, the NBB and the ECB, with the support of a Joint Oversight Team (made up of representatives of the Eurosystem NCBs), performed the official Eurosystem assessment of the MCMS's compliance with the SIPS Regulation, based on the analysis of the delivered self-assessment and underlying evidence as well as complemented by numerous iterations between MCE and the overseeing authorities. Formal exchanges between the Eurosystem and MCE were held throughout the period according to a uniform pattern applicable to all SIPS and involving Eurosystem officials and MCE personnel representing various governance levels and key operational functions. The latter encompass not only the Board of Directors and chief executive levels of MCE but also the responsible managers of internal audit, risk management, change management, IT, operations & business continuity, etc. In addition to the existing reporting of incidents, progress have been registered in the definition of an enhanced reporting of activities and major changes taking due account of the specific features of MCE.

The oversight priorities for 2023 are threefold, including (a) finalisation of the comprehensive assessment of compliance by the MCMS with the SIPS Regulation, this last step featuring the factual check by MCE and the formal adoption of the report by the Eurosystem governing bodies, (b) the assessment of MCE (based on the self-assessment of MCE) vis-à-vis the Cyber Resilience Oversight Expectations (CROE[1]) at the intervention of a joint assessment team coordinated by the NBB and the ECB, consisting of participating Eurosystem NCBs, and (c) the monitoring of the other actions planned to further improve the cyber resilience of the institution.

Most interbank retail payments in Belgium (i.e. payments for which payer and payee use accounts in different Belgian banks) are processed by the CEC, the bank-owned domestic retail payment system. Those payments include SEPA credit transfers (SCTs), SEPA direct debits (SDDs), card payments, the legacy of cheques and, on a dedicated platform launched in 2018, the instant payments. The Bank is responsible for the oversight of the CEC which takes place in the Eurosystem context on the basis of the Revised Oversight Framework for Retail Payment Systems[2] based on the PFMI. The CEC, which qualifies as a prominently important retail payment system (PIRPS), is compliant with the applicable standards.

In 2022, no major change was made in the CEC and the Bank's oversight work mostly consisted of monitoring the system. In 2023, the main focus should be on the implications of the new legislative proposal on instant payments in euros tabled by the European Commission in November 2022.

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 enable 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.

2 Available at https://www.ecb.europa.eu/pub/pdf/other/revisedoversightframeworkretailpaymentsystems201602.en.pdf.

3.2 Payment Institutions and Electronic Money Institutions

Changes in the regulatory framework

At the end of 2021, the Bank published an update of the periodic reporting requirements by payment institutions and institutions for electronic money[1]. It concerned specific additional reporting for the monitoring of the safeguarding requirements of funds received by payment and electronic money institutions from payment service users. The first report from supervised entities was received at the end of the first quarter of 2022. The objective is to obtain a clear picture of the outstanding funds on a continuous basis, in order to guarantee that in the event of a bankruptcy or other resolution reasons, the Bank, as supervisor in cooperation with the judicial authorities, can attribute all customers' funds to the rightful owners.

Due to the negative interest rates at the time, which led to an unnecessary rise in costs for the institutions under supervision, the Bank was asked for clarification on the use and scope of alternative safeguarding methods permissible under Belgian law, besides the generally applied segregation of client funds on a third-party bank account with a credit institution. The alternatives are: 1) investment in a recognised money market fund, or 2) investment in safe, liquid assets with a low degree of risk, or 3) insurance or guarantee from an insurance company or credit institution. In May 2022, the Bank published a communication clarifying the expectations of the protection of funds for the execution of payment transactions and funds in exchange for electronic money[2].

Furthermore, as a result of changes in Belgian company law, the Bank has published a Uniform Letter clarifying the existing governance rules on the composition of the legal corporate bodies. It concerns, among other things, principles regarding a majority of non-executive directors in the Board of directors, the impossibility of an employment contract for members of the Board of directors or Executive committee and incompatibilities of internal control functions with commercial/operational functions in institutions. These principles had to be fully implemented by all supervised entities by the end of 2022[3].

In May 2022, the Bank continued to provide additional clarification on certain aspects of the open banking requirements under PSD2, i.e. access to online payment accounts included in the PSD2 and the RTS SCA & CSC[4]. The aim was to resolve the last few pain points in Belgian public APIs under PSD2 and make sure they are limited to minor issues such as providing the account holder's name and refraining from using text discouraging customers from using TPP services.

Lastly, the Bank decided not to deviate from the European Banking Authority Guidelines on the limited network exclusion under PSD2 and, in June 2022, published a Circular[5] containing a faithful transposition of these Guidelines into the Belgian supervisory framework.

1 Circulars NBB_2018_31 and NBB_2019_10 dated 3 December 2021 on the periodic reporting requirements by payment institutions and institutions for electronic money.

2 Circular Letter NBB_2022_13 dated 3 May 2022 on the Protection of funds received for the execution of payment transactions and funds received in exchange for the issuance of electronic money.

3 Uniform Letter to all payment institutions, registered payment institutions, e-money institutions and limited e-money institutions dated 8 February 2022.

4 Communication NBB_2022_12 clarifications on certain aspects of in the PSD2 and the RTS SCA & CSC with regard to access to online payment accounts.

5 Circular NBB_2022_14 dated 6 July 2022 on the limited network exclusion under PSD2.

BOX 7

Need for a revision of the second payment services directive?

The revised Payment Services Directive[1], also known as PSD2, was published in the Official Journal on 23 December 2015 and applies since 13 January 2018. It was transposed into Belgian law in early 2018 by virtue of two laws[2]. The PSD2 regulates the provision of payment services in the EU and particularly sought to improve on the first Payment Services Directive, by focusing on (i) increasing payment security through the adoption of strong customer authentication and (ii) increasing competition through the creation of a no-contract right of access to payment accounts.

PSD2 introduced for the first time in EU law security requirements, in particular the requirement to apply two-factor strong customer authentication (SCA) for the initiation of electronic payment transactions and for accessing payment accounts online. PSD2 also introduced the concept of open banking, by adding to the list of payment services two new services: payment initiation services (PIS) and account information services (AIS). The former allows a licensed third-party provider (TPP) to access a payment account and initiate a payment on behalf of a payment service user (PSU). The latter allows a third-party provider to access a payment account and aggregate the data in its own application towards a payment service user or another third party.

In our FMI reports since 2019, we have written extensively on the Regulatory Technical Standards covering both these aspects, the RTS on SCA & CSC, and the work the Bank has done these past years to ensure both SCA and open banking have been successfully implemented in Belgium.

Notably, PSD2 contains a review clause requiring the European Commission to report on the application and impact of PSD2 to the co-legislators (the European Parliament and the Council), the European Central Bank and the European Economic and Social Committee. To that end, in the course of 2022, the Commission launched a review of PSD2 to which the National Bank contributed both indirectly through its participation in and cooperation with the European Banking Authority (EBA) and directly by sharing its own experience with PSD2 and making suggestions for improvements in the regulatory framework on payment services. As a result of these deliberations, the EBA published an Opinion on 23 June 2022 containing its technical advice on the PSD2 review[3].

Within the retail payments environment, most professionals seem convinced that a review might be beneficial. Besides the legal requirement for the Commission to do so, also the Bank is of the opinion that some changes to the regulatory framework on payment services could lead to substantive benefits for the users of those services as well as payment service providers. It is widely expected that the EC will propose a third Payment Services Directive by the end of the second quarter of 2023.

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 (PSD2).

2 Law of 11 March 2018 relating to the status and control of payment institutions and electronic money institutions, to the access to payment service provider activity and electronic money issuing activity and to the access to payment system and the Law of 19 July 2018 Law amending and introducing provisions on payment services in various books of the Code of Economic Law.

3 Opinion 2022/06 of 23 June 2002 of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366 on payment services in the internal market (PSD2).

The Bank would like to draw attention to four proposals it considers important for the Belgian market in relation to a revision of PSD2. These are (i) the application of SCA to AISPs; (ii) the reforming of professional indemnity insurance requirements for TPPs; (iii) reforming and detailing rules on access to a bank account (de-risking) and (iv) the publication of brand names on NCA registers.

(i) The application of SCA to AISPs

Under PSD2, SCA must be applied each time a PSU accesses their payment account online[1], including when doing so through the use of an account information service provider (AISP). In the Bank's experience, this rule has proved itself to be a major obstacle in the medium to long-term viability and, importantly, scalability of AISPs' business models. Today's PSD2 rules foresee in a voluntary 180-day exemption[2] (initially only 90 days), leaving it up to each account servicing payment service providers or ASPSP (mostly credit institutions) to make use thereof. Even though this exemption has been widely adopted in Belgium, the client churn rate that AISPs face in Belgium due to this rule remains extremely high.

The Bank feels that amending PSD2 to require AISPs to apply their own SCA, making use of security credentials they themselves provide to the PSU would remove the need for redirection of PSUs to the credit institution's interface every 180 days in order to apply SCA.

A PSU would still be required to always use SCA when accessing account information, whether doing so directly at their ASPSP (credit institution) or through an AISP's interface.

But, at the same time, there would no longer be any need for the AISP, after a first SCA with the ASPSP (credit institution), to ensure the PSU applies SCA at the level of the ASPSP (credit institution) every 180 days in order to be able to keep using its services. This would remove the client churn issue and render account information business models more viable, stable and scalable.

In the Bank's view, an important accommodating measure needs to be the amendment of the allocation of liability accordingly, with the payment service provider responsible for performing SCA, i.e. either the ASPSP or the AISP, bearing full liability towards the PSU in case of unauthorised or fraudulent access, including for data security breaches.

(ii) Reformation of professional indemnity insurance requirements

PSD2 requires both AISPs and PISPs (payment initiation service providers) to carry professional indemnity insurance in lieu of an own funds requirement[3]. The amount is calculated in line with EBA Guidelines[4] based on a formula that includes, among other things, a size-of-activity criterion based on the total value of transactions made (for payment initiation) or the number of payment accounts accessed (for account

1 Article 97(1)(a) and Article 97(4) of PSD2.
2 Commission Delegated Regulation (EU) 2022/2360 of 3 August 2022 amending the regulatory technical standards laid down in Delegated Regulation (EU) 2018/389 as regards the 90-day exemption for account access, published in the Official Journal on 5 December 2022.
3 Article 5(2) and 5(3) PSD2.
4 EBA Guidelines 2017/08 dated 7 July 2017 on the criteria on how to stipulate the minimum monetary amount of the professional indemnity insurance or other comparable guarantee under Article 5(4) of Directive (EU) 2015/2366 (PSD2).

information). The insurance is meant to cover the liability towards the payer of any erroneously executed payment initiations or errors made in the accessing of the payment account.

The Bank is of the view that this rule should be less prescriptive so as not to have a disproportionate effect on the Belgian market. It is therefore in favour of introducing a potential alternative to the professional indemnity insurance in PSD3, rendering it possible for AISPs and PISPs to opt for an alternative to insurance in order to adequately cover the risks for which they are liable under PSD2. Such alternatives could be (i) higher initial capital requirements, (ii) separate own funds requirements or (iii) different potential guarantees.

A critical reflection on the fitness for purpose of the size-of-activity criterion in the EBA Guidelines detailing the insurance requirement also ought to be undertaken.

(iii) Accessing a bank account (de-risking)

Article 36 of PSD2 stipulates that "Member States shall ensure that payment institutions have access to credit institutions' payment accounts services on an objective, non-discriminatory and proportionate basis" and that "credit institutions shall provide competent authorities with duly motivated reasons for any rejection".

Despite transposition into national law[1] and the ability for payment and e-money institutions to reach out to the FPS Economy, the Bank cannot fail to note that many payment and e-money institutions struggle to obtain or maintain banking relations with Belgian credit institutions.

The Bank is hence supportive of introducing in a PSD3 transparent criteria which avoid refusing access to or terminating an existing banking relationship for unwarranted reasons.

(iv) Publication of brand names on NCA registers

Currently, PSD2 requires the Bank to publish a register on its website containing the legal names of all licensed payment and e-money institutions[2]. This register mentions such things as the company name and the type of payment services for which that legal entity is licensed.

The Bank feels that PSD3 should introduce the obligation to also publish, for each supervised institution, the brand names under which they are offering to the market their different payment services. This would significantly increase transparency for PSUs, both customers and merchants, and assist in their assessment of trustworthy payment solutions.

1 Article VII.55/12 of the Code of Economic Law.
2 Available online on the Bank's website at https://www.nbb.be/en/financial-oversight/prudential-supervision/areas-responsibility/payment-institutions-and-electroni-5.

Ongoing prudential supervision in 2022 and priorities in 2023

The Bank's supervisory activities in 2022 consisted primarily of i) specific attention being paid to the safeguarding requirements of funds received by payment and electronic money institutions from payment service users through use of on-site inspections and off-site reporting being scrutinised and ii) the authorisation of new payment institutions, electronic money institutions and the registration of limited networks. In addition, the Bank paid specific attention to IT security policies and followed this up with on-site inspections at several payment and e-money institutions.

In 2023, the Bank intends to 1) continue monitoring of the segregation and safeguarding requirements of funds received by payment and electronic money institutions from payment service users, both on an off-site and on-site basis, 2) monitor compliance with the new governance rules as publish in the Uniform Letter as a result of the amended Belgian company law and 3) conduct audit samples on the outsourcing policies of supervised payment and electronic money institutions.

Developments in the payments institutions

Over the past year, three institutions[1] were granted a licence, one institution changed its license[2] and four institutions were withdrawn[3] from the official lists. Consequently, the number of institutions dropped slightly and stands at 39 compared to 40 last year. Including the European branches, Belgium has 47 payment institutions and electronic money institutions. On a very regular basis, the Bank is contacted by new candidates with existing or new business models, which indicates that the market is still moving, but given the slight decline, it has reached a certain maturity, explained perhaps by saturation of the Belgian market on the one hand and the Bank's stringent review of licence requirements regarding the proposed business model. Very often newly licensed institutions struggle with making their business viable due to several factors : they underestimate compliance requirements and the importance of the volume-based nature of the payments business, they start business in an existing competitive environment where incumbents maintain important stakes and which adapt continuously their service offering.

In the card-payments-acquiring landscape, competition is ever growing mainly through international players. This is reflected in the increasing number of European branches. The number of branches has risen from three in 2017 to currently eight, which mainly focus on facilitating online card payments for merchants. From recent contacts with candidate branches, this trend is likely to continue in 2023.

With regard to the business models of new service providers, the bank notes an increase in the request for limited network exclusions. This originates in part from virtual asset providers such as crypto-currency exchanges. In addition to their virtual asset activities, these institutions often provide wallet services which fall under the exclusion status as intended under PSD2. Another source of the increase in limited network exemption requests lies in the mobility services, with examples such as ridesharing, e-mobility and toll solution providers seeking exemption status.

The Bank continues to note that some Belgian banks or financial institutions have ended their cooperation with payment institutions offering money remittance services. As a result, these institutions have had to look for alternatives.

Due to the relocation of payment institutions, as a result of the Brexit, the Belgian money remittance landscape has changed profoundly. A number of world players in terms of money remittance have decided to relocate to

1 Odoo Finance NV, Freedelity SA and Atlantic Money NV.
2 Cake NV.
3 Together Connected NV, PagoFX Europe NV, Let's Didid NV, GuiSquare NV.

Belgium, with the result that the volume of transactions processed via Belgian payment institutions has risen considerably.

The following figures demonstrate the impact of Brexit on the money remittance market. At the end of 2019, the total amount of incoming and outgoing money transfers in Belgium via money remitters was € 1 546.8 million, of which 37.7 % was processed via Belgian payment institutions and 62.3 % through other EEA payment institutions, active in Belgium. By the end of 2022, the money remittance volume of Belgian money remitters (and EEA money remitters active in Belgium) rose to € 17 304.8 million of which 97.1 % was processed via Belgian payment institutions.

At the end of 2022, nine Belgian payment institutions provide money remittance services and four of them operate an agent network with a total of more than 10 000 agents (of which approximately 90 % Moneygram International agents) across the EEA. In Belgium, nearly 2 000 active money remittance agents are present, of which approximately 75 % agents of other European payment institutions and 25 % agents of Belgian payment institutions. Based on the data from the EBA register, there are just over 120 000 active agents in the EEA.

BOX 8

MICA

As part of its Digital Financial Strategy[1], and as explained in the Bank's previous Financial Market Infrastructure Report (2022)[2], the European Commission is continuing its work on the implementation of its new regulatory flagship in the payments eco system : the Markets in Crypto- Assets Regulation (MiCA).

Preliminary agreements were reached by the Council and the European Parliament in the third and fourth quarters of 2022 on a proposal for an EU Regulation on crypto-assets. This legislative proposal feeds into a "*crypto ecosystem*" already more than 10 000 projects strong. In fact, more and more wealth is now being invested not only in Bitcoin, but also in many other more or less well-known crypto-assets. However, these assets are not always successful, as illustrated by the numerous bankruptcies (e.g. Celsius Capital, FTX, BlockFi and Three Arrows Capital), scandals (e.g. the Bitfinex exchange hack) and frauds (e.g. pump and dump schemes) that have repeatedly rocked this ecosystem. Furthermore, the lack of transparency (especially regarding liquidity and reserves) as well as professionalism and protection for investors and users is rampant in this field[3].

The European Commission's objectives behind MiCA are therefore manifold, starting with providing legal certainty on crypto-assets within the European Union. The difference in treatment of these assets between the different European states and the intermingling of pre-existing laws applying to some extent to this "*crypto ecosystem*" did require a response in line with the challenge. Furthermore, this Regulation also seeks to stimulate innovation by giving the ecosystem some space, while ensuring that the other side of the medal, i.e. consumer protection and market integrity, is not left out. Indeed, investor/consumer

1 For further details, see Digital finance package (europa.eu), ECB, 2020.
2 For further details on this part, consult fmi-2022_dlt.pdf (nbb.be), NBB, 2022.
3 For more details, please refer to the joint FSMA and NBB warning on the use of crypto-assets cp140114en.pdf (nbb.be).

protection and the extension of some key principles in these fields to the "*crypto ecosystem*" is a key objective of MiCA. Finally, even though crypto-assets do not yet pose financial stability issues as the total value of their ecosystem is not significant (as compared to the market capitalisation of traditional finance), this aspect is being analysed continuously by regulators worldwide and MiCA is a step in the right direction.

To go into more detail on the legislative draft and as a reminder of what has previously been stated[1], among the three categories of crypto-assets that MiCA consider as part of its scope, two of them are defined as "*stablecoins*". Indeed, the Regulation's interest in these crypto-currencies is motivated by three main concerns. First, the ability of these stablecoins to potentially be backed by one or more traditional fiat currencies has drawn the attention of the European Commission to the subject. Secondly, their wider use (compared to other crypto-assets) as a medium of exchange, avoiding the volatility experienced by currencies such as bitcoin, has raised alarm bells. Finally, the risks associated with crypto-currencies, which are not dissimilar to those mentioned above, have added to the sense of urgency. Indeed, once investor confidence in the issuer's liquidity reserves is lost, these assets can also lose their value at lightning speed (e.g. Terra/Luna stablecoins).

Therefore, to return to the scope of regulation, MiCA addresses these risks by first identifying two types of stablecoins. On the one hand, electronic money tokens (EMT), whose value is determined by reference to the price of one official currency, and on the other hand, asset-referenced tokens (ART), by referring to the value of several fiat currencies, one or several commodities or one or several crypto-assets, or a combination of such assets (e.g. X8C – backed by a basket of eight major currencies and gold). Issuers of these two categories of stablecoins are subject to multiple rules. Key among these is that prior to being allowed to offer such a stablecoin in the EU, the issuers will have to notify their national competent authority (NCA) through a White Paper – subject to NCA approval in the case of an ART – and publish it, thus ensuring transparency and accountability towards the investing public. Other notable rules relate to the investment by these issuers of funds received, the reserve of assets, redemption rights for investors, consumer/investor protection, marketing rules and liability.

The third category of crypto-assets included in the new Regulation includes remnant forms of the "*crypto ecosystem*" under the term "*residual crypto-assets*", which corresponds to but is not limited to e.g. Bitcoin, Ether, utility and loyalty tokens, etc. These assets, whose value depends on their own architecture, will be subject to a "light" regulatory regime (except for crypto-assets already on the market). This involves a simple registration requirement with the NCA rather than ex-ante notification or approval, the publication of a white paper for which they are legally responsible, and strict conditions regarding their marketing to ensure an adequate level of consumer protection.

Besides seeking to regulate issuers of crypto-assets, MiCA also puts so-called crypto-asset service providers (CASP) in its scope as they are considered by the European Commission as the gateway towards traditional finance. As defined in the Regulation, CASPs are any legal entity that provides one or more crypto-asset services[2] in a professional capacity. Along with the extension of existing rules in

1 For further details on this part, consult fmi-2022_dlt.pdf (nbb.be), NBB, 2022.

2 These services include but are not restricted to the custody and administration of crypto-assets on behalf of third parties, the operation of a trading platform for crypto-assets, the exchange of crypto-assets, the execution or reception and transmission of orders for crypto-assets on behalf of third parties and the provision of advice on crypto-assets.

the payments and securities sector (e.g., outlawing market abuse such as frontrunning) and rules specific to the service provided by each CASP, they will be required to comply with rules related to governance, prevention of conflicts of interest, outsourcing, and how crypto-assets may be invested. On a side note, it should be mentioned that, unlike CASPs, most non-fungible tokens are not included in the scope of MiCA, as they will be studied in a more targeted way by the European Commission in the coming years.

As regards the implementation of the legislation[1], the European Supervisory Authorities[2] and the competent national authorities (hereinafter referred to as NCAs) will be responsible. On the one hand, the European Banking Authority will be in charge of the supervision of significant EMTs and ARTs[3] while the European Securities and Markets Authority will become responsible for producing regular reports and providing feedback to the Commission, building and maintaining a register with information about crypto-assets white papers, issuers of EMTs and ARTs, and ensuring coordination and cooperation between NCAs. These NCAs will in turn be responsible for overseeing non-significant EMTs and ARTs as well as CASPs, with the possibility of suspending their service offering, publicising the fact that a certain CASP is not compliant, suspending advertisements, inviting auditors, imposing fines and banning members of the management. In addition, NCAs will also ensure market surveillance by preventing practices such as market manipulation or insider trading.

Regarding the further course of action for the legislation, the launch of the second step of implementation (EU financial services regulatory process[4]) started early this year. This step allows the Commission to adopt, adapt and update regulatory technical standards and guidelines with the help of advisory bodies composed of representatives of EU countries and competent European supervisory authorities. In the case of MiCA, the EBA and the ESMA have been tasked with developing draft regulatory technical standards and guidelines to be adopted across the European economic area. In EBA's 2022 assumptions[5], they will have the responsibility of drafting approximately 18 RTSs and GLs by 2024, while ESMA indicates that it is expected to deliver "*a significant number of guidelines and technical standards in 2023 and 2024 – many in close cooperation with EBA*[6]". Finally, although the Bank's regulatory role under MiCA has not yet been fully defined, it is expected that the Bank will play an important role in this reflection and drafting process.

1 A partial implementation for all aspects related to EMTs and ARTs is planned in the Spring of 2024, and the final implementation (including CASPs) in the Autumn of 2024.
2 Which are in this case the European Banking Authority and the European Securities and Markets Authority.
3 To consult the conditions for an EMT/ART to be considered significant, see Markets in crypto-assets (MiCA) (europa.eu), European Parliament, 2022.
4 For further details, see Regulatory process in financial services (europa.eu), European Commission.
5 For further details, see 2023 EBA Work Programme.pdf (europa.eu), EBA, 2022.
6 For further details, see AWP 2023 (europa.eu), ESMA, 2022.

BOX 9

CBDC

Together with the European Central Bank, the National Bank of Belgium is pursuing the preliminary work for the potential introduction of a digital euro, the main objectives of which would be to further stimulate the digitalisation and efficiency of the European economy while strengthening the strategic autonomy of the euro area without competing with private payment solutions. The Eurosystem is thus currently working on the investigation phase, which started in October 2021 and will last until September 2023. During this phase, the Eurosystem will seek consensus on technical questions and study the implications of the issuance of a digital currency on payment infrastructures, financial stability and financial inclusion.

As a reminder, consultation rounds and focus groups have been held with citizens of the euro area throughout 2020 and 2021[1]. Moreover, a regular dialogue on a digital euro has been established with all market participants[2], including banks, other payment service providers, consumer representatives and merchants through the Market Advisory Group (MAG) or the Euro Retail Payments Board (ERPB) at European level and the National Retail Payments Committee (NRPC) at Belgian level. The national central banks are also heavily involved in the investigation process, both through participation in the High-Level Task Force (HLTF – CBDC) and the Project Steering Group (PSG). The HLTF is responsible for taking major decisions on the functionality and intrinsic characteristics of the digital euro, whereas the PSG coordinates the study and research efforts of both national central banks and the ECB. The joint work of both, linked to the insights gained from the consultations and the various focus groups, has thus enabled progress to be made in the design of a potential digital euro.

One of the main decisions taken so far concerns the "transfer mechanism", i.e. the procedure by which transactions and their validation are carried out. As such, the Eurosystem has approved the further exploration of an "online third-party validated solution" and an "offline peer-to-peer validated solution". The first (online validated transaction by a trusted authority) is similar to transfers via commercial banks while the second one is similar to transactions performed between two individuals using their smartphone (or other devices) without being in an online internet modus (i.e. like a cash transaction). However, the time to market for the latter solution is more uncertain due to its reliance on NFC or similar hardware-based technologies. The development of the first "online third-party validated solution" will not be delayed if the timely delivery of a validated peer-to-peer solution for offline payments proves unfeasible.

In addition, regarding the settlement model and the role of intermediaries, it was decided that transactions would be settled at Eurosystem level for online transactions and at the local storage device level for offline transactions. Transaction management tasks would be carried out by supervised intermediaries (credit institutions or payment service providers), who would be the direct contact entities for private individuals, merchants and companies using digital euro in their role of depositories of the contractual account management relationship with the end user.

1 See "Digital euro: listening to the public (europa.eu)", ECB, 2022.
2 See "Digital euro Project governance and stakeholders (europa.eu)", ECB, 2022.

Another crucial feature of the digital euro according to the public[1] is privacy and it has also been the subject of thorough reflections over the past few months. While initially, in a baseline scenario, it was considered to mirror current AML/CFT practices of private sector digital solutions, it was decided that the Eurosystem would explore two additional options, diverging from these practices in favour of more privacy (while not impeding the appropriate exercise of AML/CFT controls). These options are (i) selective confidentiality for low-value online payments and (ii) an offline functionality which ensures that the users' balances and transaction data remain private. Further work is still needed to explore how both options could be activated, either under the current regulatory AML/CFT framework or under a new tailored regime. In addition, various privacy-enhancing technologies are being tested for the online solution.

Finally, a significant step toward financial stability taken recently is the exploration of tools to control the potential amount of digital euros in circulation. Indeed, if held by users in large volumes, a digital euro could lead to a structural substitution of commercial bank deposits, which could have an adverse impact on monetary policy, financial stability and credit flow within the real economy. To quote Marcus Brunnermeier: "*the digital euro should be present everywhere but important nowhere, should be successful but not too successful*"[2]. As such, several mechanisms to prevent the rise of such adverse effects were discussed. These include quantitative limits and remuneration-based tools, for instance. The former is able to limit the individual use and speed of conversion of deposits while the latter could reduce the attractiveness of digital euro holdings beyond a certain threshold compared to other highly liquid and low-risk assets. Both tools will be included in the design of a potential digital euro so that the relevant tool and settings thereof can be defined closer to the time of issuance. Which will then give the opportunity for the Eurosystem to consider the actual economic, financial and monetary policy environment (e.g., interest rates, the level of excess reserves, etc.) and keep the necessary flexibility in the future. In addition, the Governing Council agreed on the possibility of using a so-called "*waterfall*" functionality, whereby funds in the digital euro wallet exceeding the holding limit would be automatically transferred to a linked commercial bank account. The inverse functionality (namely "*reverse waterfall*") will ensure that end-users can make a payment even if the amount exceeds their current digital euro funds, by taking additional liquidity from the user's linked commercial bank account. Both features, activated at the discretion of the end-user, will ensure a seamless payment experience, thereby preventing the holding limit from becoming a transaction limit.

On top of the above-described decisions in relation to the design of a potential digital euro, in-depth work is also taking place, in relation to the development of a prototype for a digital euro (centralised back-end infrastructure) and the collaboration with selected market players for the construction and design of several user interface prototypes (front end infrastructure) according to the wide range of usage scenarios for which the digital euro will be usable, e.g. peer-to-peer online transactions (CaixaBank), peer-to-peer offline transactions (Worldline), e-commerce transactions (Amazon), point-of-sale payments in physical shops (initiated by the payer – EPI[3]: initiated by the payee – Nexi). It should be noted that transfers to governments and from governments are also part of the list of use cases prioritized by the ECB. However, no front-end infrastructure prototype is currently being studied or tested for such use cases.

1 See "Eurosystem report on the public consultation on a digital euro (europa.eu)", ECB, April 2021.
2 See "The digital euro: policy implications and perspectives (europa.eu)", Markus K. BRUNNERMEIER, Jean-Pierre LANDAU, 2022 (p8).
3 European Payments Initiative.

The user interface prototype development exercise serves as a learning exercise, results thereof are expected in the first semester of 2023 and will be published). There are no plans to re-use the prototypes in later phases (e.g. realisation) of the Digital Euro project.

Furthermore, the ECB is also working on a draft of a digital euro scheme rulebook, i.e., a set of rules for payment transactions with a digital euro. This approach is considered to be the most efficient way to achieve the objectives of a digital euro and to capitalise on the respective strengths of the public and private sectors. Indeed, a specific scheme would establish a set of common rules, standards and procedures that would ensure pan-euro area reach and promote a harmonised end user payment experience, as certain requirements on commercial elements could be specified and give significant flexibility to respond to end user preferences and specificities. A scheme rulebook manager was appointed at the beginning of December 2022 (Christian Schäfer) to set up and coordinate the Rulebook Development Group, composed of representatives of the Eurosystem national central banks and market participants (including consumer delegates).

Finally, in parallel with this report, the Eurosystem continues to actively engage with all stakeholders, with new round of focus groups planned around prototype completion during the remainder of the investigation phase. The Eurosystem will decide in autumn 2023 whether to proceed to the preparation phase. Meanwhile, the European Commission intends to come up with the legislative groundwork necessary to implement a digital euro in the second quarter of 2023.

3.3 Payment transaction processors

Changes in the regulatory framework

In 2022, the Belgian regulatory framework applicable to payment transaction processors remained unchanged.

Prudential & oversight approach

In 2022, one new entity (Worldline Switzerland ltd) providing processing services in the Belgian payments market was designated as a systemically important payment processor for the Bancontact scheme. Table 2 shows the entities that have the status of systemically important processor of payment transactions based on Article 6 of the Law of 24 March 2017 on the oversight of payment transactions processors and the scheme(s) for which they have such status.

Table 2

List of systemically relevant payment processors

(as at 31 December 2022)

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

Source: NBB.

Systemically important processors must comply with requirements that aim to maintain the stability and continuity of retail payments in Belgium, e.g. the compulsory comprehensive risk management in the fields of detection, appraisal and development of mitigation measures. The legal framework for payment transaction processors also includes a strict process for incident reporting to the Bank and enables the latter to apply a sanctions regime. The Bank's oversight of such processors focuses on cyber resilience and operational reliability.

3.4 Card payment schemes (CPS)

Regulatory framework

In November 2021, the Eurosystem published a new oversight framework designed to foster improvements in the soundness and efficiency of electronic payments. This new oversight framework for electronic payment instruments, schemes, and arrangements (PISA Oversight framework) is based on the internationally agreed Principles for Financial Market Infrastructures (PFMI). It is now the benchmark for Eurosystem oversight of

payment instruments, schemes and arrangements, and replaces the former standards used by the Eurosystem[1]. The PISA oversight framework was designed with the objective of addressing technological developments in the payment industry. The framework[2] itself is complemented by an assessment methodology[3] and an exemption policy[4]. This policy aims at identifying schemes and arrangements of a certain importance and level of risk based on specific criteria relating to the size of the user population, market penetration in terms of value and volume, and geographic relevance. Only those schemes and arrangements will have to comply with the requirements of the framework. In Belgium, this concerns Mastercard Europe and Bancontact. Like all companies that are already subject to Eurosystem oversight, both card payment schemes were expected to adhere to the principles of the new framework by 15 November 2022. The conformity of the relevant entities with the framework will be assessed by the Eurosystem from 2023 on.

Oversight priorities / activities in 2022

The Belgian domestic CPS, Bancontact, is subject to oversight by the Bank. In 2023 Bancontact will be assessed against the PISA framework. In 2022, the Bank had already intensified its dialog with the scheme in that respect. The assessment process is based on a documented self-assessment provided by the scheme which will be discussed, reviewed and, where needed, amended and detailed by the Bank which is responsible for the evaluation of the compliance level. Prior to its finalisation, this assessment report will be submitted to other central banks of the Eurosystem in order to be challenged in a peer review.

For MCE, which qualifies both as a CPS and as a SIPS, and with a view to avoiding duplication of tasks, the new PISA framework provides for account to be taken of the results of every oversight duty performed during the monitoring of its continuous compliance, as a SIPS (see section 3.1) with the requirements of the SIPS Regulation.

In practical terms, a review was carried out in 2022 to determine which parts of the PISA framework assessment methodology have not yet been addressed by the comprehensive assessment of the MCE's compliance with the SIPS Regulation. The assessment of MCE's compliance (as a CPS) with the PISA framework should kick-off at the 2023 Q2-Q3 horizon, ideally when the CROE assessment will be close to completion.

1 These standards include:
- The harmonised oversight approach and oversight standards for payment instruments (ECB, February 2009);
- The oversight framework for card payment schemes (ECB, January 2008);
- The oversight framework for direct debit schemes (ECB, October 2010);
- The oversight framework for credit transfer schemes (ECB, October 2010);
- The "Electronic money system security objectives" (ECB, May 2003).

2 Available at https://www.ecb.europa.eu/paym/pdf/consultations/ecb.PISApublicconsultation202111_1.en.pdf.

3 Available at https://www.ecb.europa.eu/paym/pdf/consultations/ecb.PISApublicconsultation202111_2.en.pdf.

4 Available at https://www.ecb.europa.eu/paym/pdf/consultations/ecb.PISApublicconsultation202111_3.en.pdf.

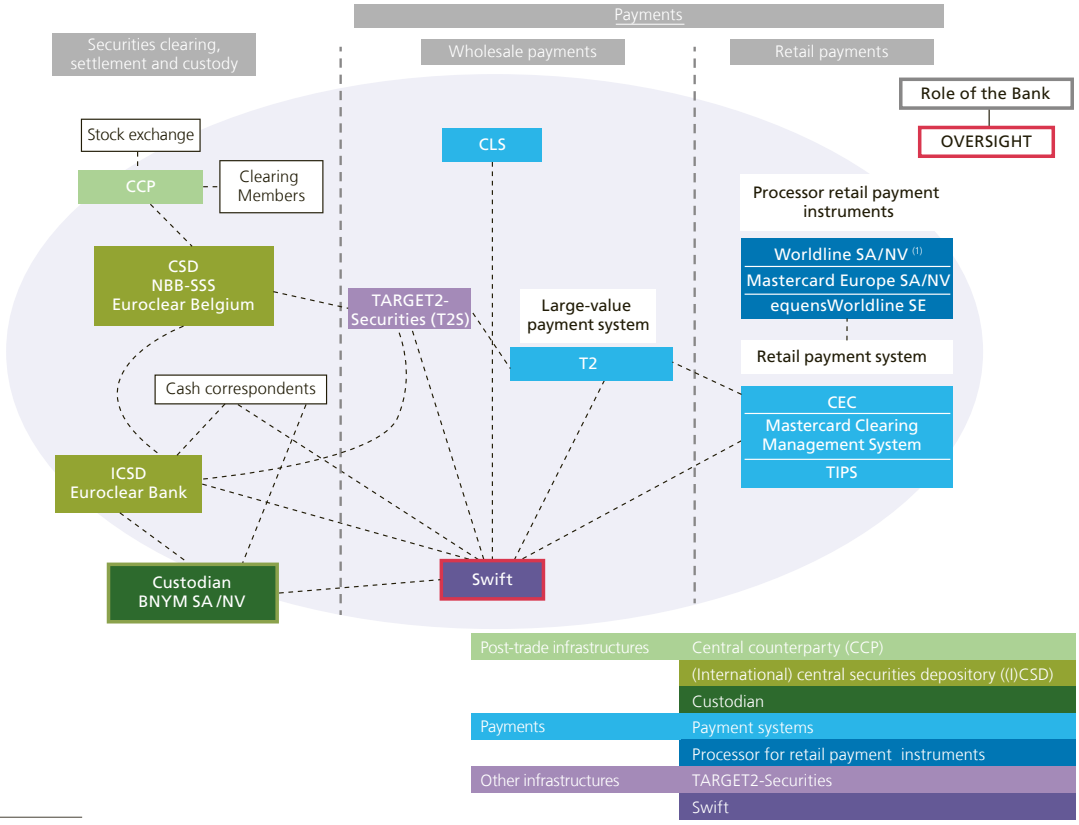
4. Swift

The Society for Worldwide Interbank Financial Telecommunication (Swift) is a limited liability cooperative company that provides messaging services to financial institutions and market infrastructures across the globe. Swift serves different customer types which vary in terms of size and activity: banks, brokers, investment managers, fund administrators, custodians, corporates, and treasury counterparties. Swift is registered in Belgium with its headquarters located in La Hulpe.

Through its financial messaging services, Swift fulfils a crucial role in facilitating correspondent banking and financial market infrastructure activities. Such a fundamental role for the global financial industry creates significant systemic dependency on Swift. Hence, the G10 jurisdictions established the cooperative Swift oversight framework to monitor Swift's activities with the aim of safeguarding financial stability.

Chart 4

Swift as a critical service provider to the financial industry



1 Only the Belgian activities of equensWorldline SE are overseen by the NBB. Worldline Switzerland ltd is also designated as systemic processor for its switching activities for Bancontact according to the Law of 24/03/2017 regarding the oversight of payment processors and has specific obligations in that framework but it is not overseen by the NBB.

4.1 Swift oversight framework

4.1.1 Swift and its users

National member groups are represented by Swift's users and are organised per jurisdiction. These users own and control the company and are involved in the appointment of Swift Board members. Swift's share distribution is based on the message traffic, ensuring that the Board represents the jurisdictions with the largest users, i.e. with the highest message traffic volumes. Since message traffic proportionality is not static, the shares are reallocated every three years to mirror the actual Swift user community. In 2021, such a redistribution took place but did not result in the introduction of any new jurisdictions on the Swift Board. The next share reallocation is scheduled for 2024.

Swift provides messaging services to customers from more than 200 countries, amounting to approximately 11 600 Swift users. The following numbers reflect Swift's global presence: in 2022 11.3 billion messages were sent with a daily average of 44.8 million messages. Despite the global geopolitical tensions and economic uncertainty, Swift achieved a year-over-year growth of FIN traffic of 6.6 % by the end of 2022. The main contributors to this growth were the economic recovery and the securities market volatility, sparked by higher volumes of securities settlement instructions.

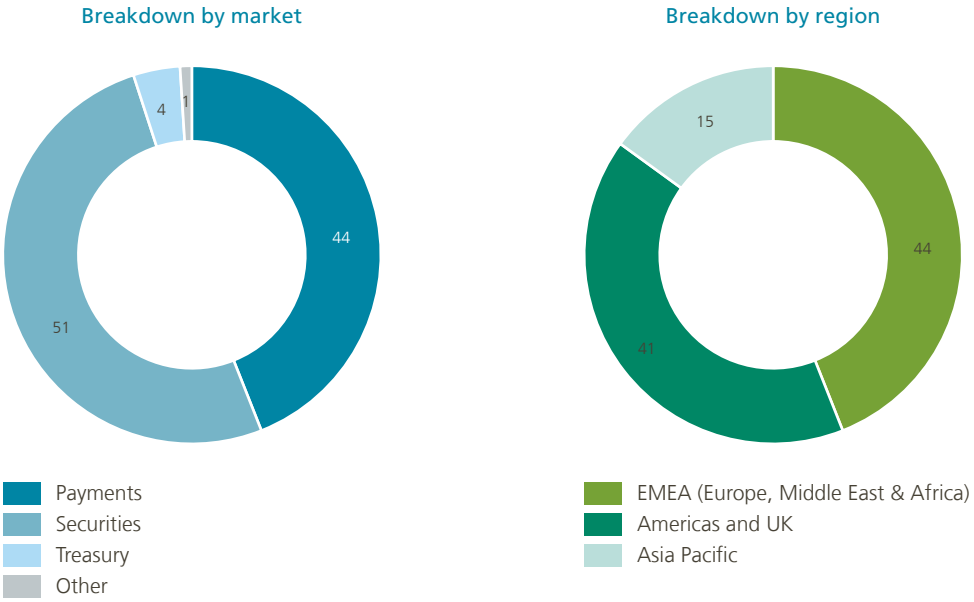
The core messaging service for exchanging financial messages is Swift's FIN application. The figure below depicts Swift's FIN traffic for 2022 distributed per region and market. There was a total of 11 696 live users, of whom 2 360 are Swift's shareholders belonging to different national member groups. In line with figures for previous years, the payments (44.4 %) and securities (50.8 %) markets represented the lion's share of Swift's messaging for 2022. The Europe, Middle East and Africa (EMEA) region claimed the largest part of the total 2022 FIN traffic volume, closely followed by the Americas and UK region.

It is worth noting that, for the ISO 20022 migration for cross-border payments and cash management, use of the FIN messaging service will gradually give way to the FIN Plus service (or InterAct service). A co-existence period, during which users will be expected to switch from the legacy FIN MT to the new ISO 20022 MX format, started in March 2023 and ends in November 2025.

Chart 5

Swift FIN traffic distribution by region and market

(2022)



Source: Swift.

4.1.2 International cooperative arrangement

In 1997, the G10 central banks formalised the Swift oversight arrangement for the purpose of monitoring the adequate and safe functioning of the critical service provider. In addition to the participating G10 jurisdictions, the Bank for International Settlements and the European Central Bank are represented in the international working groups. As Swift is headquartered in Belgium, the NBB is the standing lead overseer and chairs the international oversight meetings.

The G10 central banks are represented in the four working groups: the Technical Group (TG) which conducts technical fieldwork, the Cooperative Oversight Group (OG) which is the decision-making body and sets the oversight strategy, the Executive Group (EG) which serves as the interface for overseers to communicate conclusions and recommendations to Swift's Board and Executive Management, and the Swift Oversight Forum (SOF) which involves a wider group of central banks discussing the oversight activities and relevant changes at Swift.

Given the systemic character of Swift, a wider group of G20 jurisdictions are also directly involved in the oversight. These G20 central banks are represented in the SOF working group. Their membership corresponds to their share in the total Swift traffic volume and the CPMI membership composition. The SOF deals with the Swift oversight conclusions, planning and priorities, Customer Security Programme and discussions on dedicated topics.

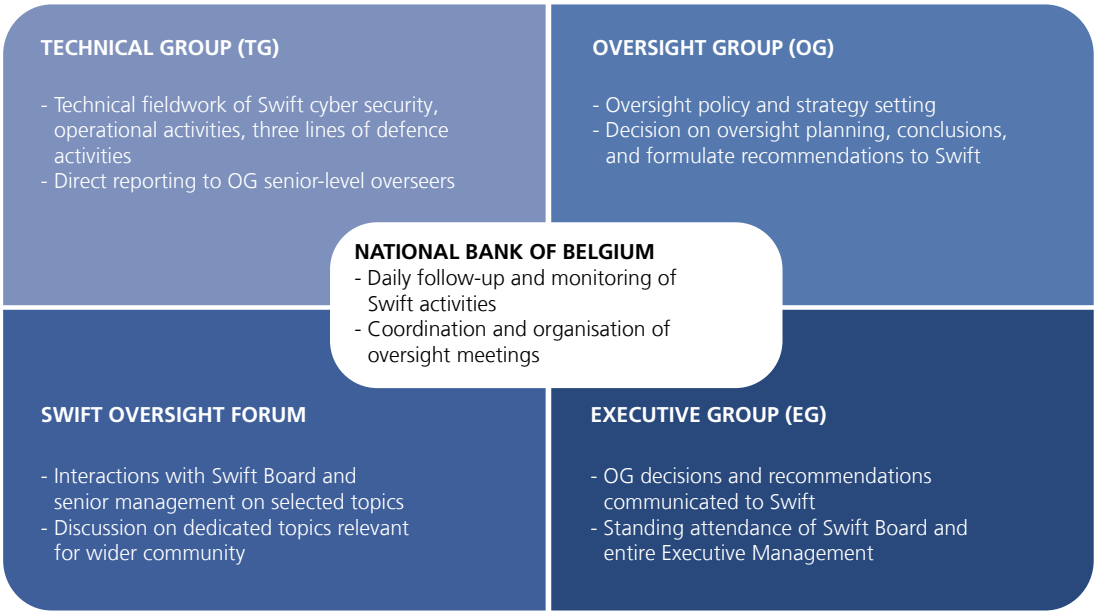
In its capacity as Swift's lead overseer, the NBB has a dedicated team which conducts daily monitoring and follow-up of Swift's activities and projects. As formulated in the Swift Oversight Protocol, the NBB serves as the entry point for channelling information to the other overseers and, as chair, coordinates the different working groups in terms of reporting to the other overseers and preparing discussion items for them.

More detail on the composition and scope of activities for each of the working groups can be found in earlier editions of the Financial Market Infrastructures and Payment Services Report (2017-2021).

The following figure gives an overview of the different working groups involved in the Swift oversight.

Figure

Swift oversight working groups involving G10 and G20 central banks



The oversight on Swift is based on the five high-level expectations (HLEs), i.e. (i) Risk Identification and Management, (ii) Information Security, (iii) Reliability and Resilience, (iv) Technology Planning, and (v) Communication with Users. These five HLEs were set out in Annex F to the CPMI-IOSCO's Principles for FMIs and form the oversight expectations applicable to all critical service providers to FMIs.

The overseers' review activities are all rooted in the five HLEs and drive the oversight planning and priorities. Overseers assess the adequacy of Swift's management of operational and security risks across the three lines of defence (LoDs) by comparing it with these expectations. Swift is thus expected to adhere to the HLEs through appropriate reporting to overseers (i.e. the provisioning of required documentation, interactions with Swift's three lines of defence, and discussions with Executive Management and Board).

More details on the specific description of the five HLEs can be found in earlier editions of the Financial Market Infrastructures and Payment Services Report (2017-2021).

4.2 Selection of major topics reviewed by overseers in 2022

This paragraph covers a non-exhaustive selection of major topics which overseers analysed in 2022. The highlighted topics are a sub-set and not a full representation of the review work conducted in 2022 (e.g. standing topics such as business continuity exercises, effectiveness of three lines of defence, enterprise risk management, and internal audit activities).

4.2.1 Messaging traffic

With 2022 being marked by severe geopolitical unrest and economic uncertainty, as explained in box 10, overseers were keen to analyse the impact of these factors on the growth of Swift's messaging traffic. The fact that Swift could still present high year-to-date traffic growth demonstrates the trust that the global financial community continues to place in the company.

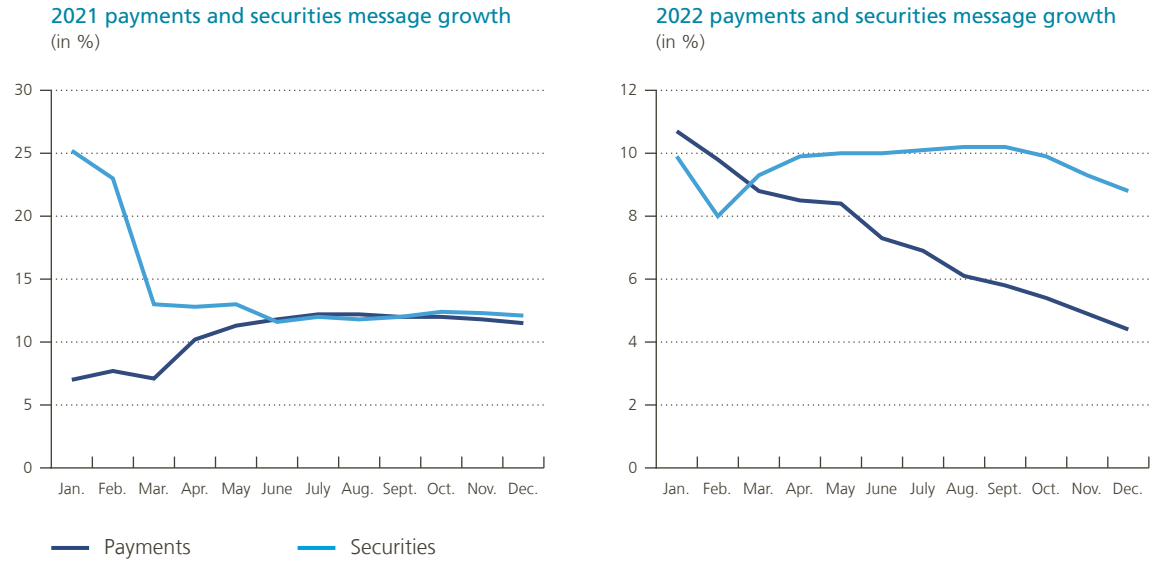
In 2021, there was a marked increase in payments traffic via Swift's network, which could be attributed to the positive outlook following a prolonged period economic uncertainty due to the pandemic. In 2021, Swift's payments traffic grew by 11.5 % compared to 2020 and securities traffic was up by 12.1 % on 2020. Overall, FIN activity recorded 11.4 % growth in 2021.

Given the new challenges posed in 2022 due to the geopolitical tensions, as well as energy crisis and inflationary worries, Swift was still able to provide some solid growth figures. There was strong growth for both payments (4.4 %) and securities traffic (8.8 %), contributing to an overall FIN traffic growth of 6.6 % for 2022.

The following two graphs show the percentage changes in payments and securities traffic growth for 2021 and 2022. Over the course of 2021, growth of payments and securities traffic converged, with both markets recording stable, double-digit growth from mid-2022. The more favourable economic outlook following the COVID-19 pandemic might have been a driving factor for this development. For 2022, Swift maintained positive growth for both payments and securities traffic. Securities traffic posted a growth trend of about 10 % throughout the year, whereas for payments there seemed to be a slight decline in traffic throughout 2022.

Chart 6

Growth of payments and securities message traffic in 2021 and 2022



Source: Swift.

4.2.2 Cyber and physical resilience

Over the course of 2022, Swift regularly reviewed the resilience measures in place, both from a cyber security perspective and from a physical security perspective, ensuring vigilance and readiness in light of any present or future geopolitical tensions. The overseers also stepped up their monitoring of Swift's operations, with weekly updates being provided to overseers up until the end of 2022.

The year 2022 also marked a period of severe turmoil and uncertainty on the energy markets, leading to some countries drafting shutdown plans and reviewing mitigating measures for their critical infrastructures. Viewed as power supply is crucial for the proper functioning of Swift's control centres and datacentres, and thus for the functioning of the global financial markets, this subject also received appropriate attention by overseers. Data integrity and redundancy measures were reviewed, as well as a number of mitigating measures in place, such as uninterruptable power supplies (UPS) and back-up generators and the required fuel supplies.

4.2.3 Customer Security Programme

The Customer Security Programme (CSP) has been a recurring topic on the overseers' agenda ever since the programme was introduced following the 2016 Bangladesh case. Swift has built up an extensive programme enhancing its users' cyber security, their counterparts, and the entire community. Through the CSP, users are required to adhere to certain controls and good practices to appropriately secure their on-premises IT environments connecting to the Swift network. With cyber-attacks continuing in the financial sector, overseers are seeking reasonable assurance on the effectiveness of the CSP and corresponding initiatives, designed to adapt to new threats, improve cyber security capabilities, and adhere to regulatory expectations.

Over the years, Swift has taken multiple initiatives and improved various aspects of the CSP, such as the yearly review of the Customer Security Control Framework (CSCF), improvements to the Know-Your-Customer (KYC)

tool, launch of an Independent Assessment Framework (IAF), introduction of mandated assessments, more effective involvement of supervisors, actionable updates on the Information Sharing and Analysis Centre (ISAC) portal, and organisation of recurring awareness campaigns. Thanks to these actions, Swift has informed overseers that there has been a downward trend in customer cases. In fact, for the first time since the inception of the programme, no fraudulent messages have been sent over the Swift network during both 2021 and 2022. Additionally, not a single customer case was reported during 2022, demonstrating the CSP's effectiveness. On account of its successful track record and promising results, Swift is expected to continue to enhance the programme.

One such expectation concerns the involvement of supervisory authorities in using the CSCF self-attestation data of financial institutions. From the outset, overseers have encouraged Swift's move to engage supervisors more directly in making effective use of the rich self-attestation data of its users, which could provide crucial input for supervisors' risk-based planning and scoping. The identification and onboarding of the relevant supervisory authorities in the Know-Your-Supervisor (KYS) tool have proven to be challenging because some jurisdictions have multiple supervisory authorities relevant for one country. According to Swift's first reporting to overseers on the use of the self-attestation data by the onboarded supervisory authorities for financial institutions within their relevant jurisdictions has fallen short of expectations. Overseers have stressed the importance of this entire initiative and will continue to monitor the actions required to improve the supervisory onboarding and safeguard the effectiveness of the KYS application.

As per standard procedure, overseers contributed, together with the national member groups, to the yearly review of the Customer Security Control Framework (CSCFv2023), which resulted in one advisory control being turned mandatory, as well as a number of other changes to the framework:

i. Promotion of the "advisory" control "1.*5 A Customer Environment Protection*" to "mandatory", with the objective of further aligning Swift's different architecture types, as well as protecting all connectors within different architecture types consistently;
ii. Introduction of a lighter attestation regime for Receiving-Only users. Over 1 100 active BICs have been identified by Swift as only receiving files or messages, not emitting any (potentially fraudulent) messages. Examples are corporates using reporting or dashboard applications. For these users, the recurring CSP compliance with Independent Assessment has become a costly annual exercise while representing minimal risk to process fraudulent transactions. This is why Swift proposes a lighter version of the CSP for Receiving-Only users. The requirement for this is that users will have to declare being a Receiving-Only institution, after which Swift will centrally implement controls to prevent any message or file being sent from their BICs. After this procedure, the user in question will still have to provide an annual attestation but will be exempt from the Independent Assessment.
iii. The method of indicating compliance to the CSCF has been simplified to bring it in line with other security frameworks and industry practices. Institutions and participants can now indicate compliance by checking a single check box, with the option to include written comments in a text box.

Swift users are expected to comply with the mandatory security controls (i.e. security baseline) and can also attest their compliance with the advisory controls (i.e. good practices for securing local IT infrastructures). A user's self-attestation (i.e. compliance with the CSCF security controls) is uploaded to the Know-Your-Customer Self-Attestation (KYC-SA) tool by the end of each year. The new CSCF version (v2023) was introduced in mid-2022, and users have until the end of 2023 to submit their attestations.

By 31 December 2022, 87 % of Swift customers had provided a valid CSP attestation, and of these self-attestations 79 % of customers indicated compliance with all mandatory controls. The compliance levels and the number of self-attestations are in line with the uptake in 2020 and 2021. Through Swift's quality assurance and monthly metrics reports, overseers closely monitor various CSP-related metrics, such as the users' attestation and consultation levels. The reporting on CSP metrics is crucial for overseers to obtain a view of the cybersecurity stance of the Swift user community. As such, overseers expect Swift to refine and extend the CSP reporting metrics as appropriate.

The Independent Assessment Framework (IAF), which was launched in mid-2021, requires all Swift users to perform a Community Standard Assessment to further enhance the accuracy of their attestations. Every Swift user has to have their attestations independently assessed through either an internal independent assessor (e.g. the second or third line of defence) or by an external independent assessor (such as a consultancy firm). Users are free to select the internal and/or external resources to conduct the assessment. If a user still opts for a self-attestation without the independent internal or external assessment; they will be considered as non-compliant to the CSP.

Initial reporting on compliance to the IAF looks promising, with 96 % of users indeed opting for an independent assessor, and thus remaining compliant with CSP requirements. Of these users, about half opt for an independent internal assessor, while the other half opts for independent external assessors. The percentage of Swift traffic sent by BICs who provide attestations supported by an independent internal assessment or an independent external assessment is fairly constant at 99 %.

Overseers also assess Swift's processes for communication with its users regarding the use of new technologies, fraud cases, and common cyber security threats affecting the community. Swift's Information Sharing and Analysis Centre (ISAC) provides its users with actionable information on cyber threats, indicators of compromise and common hacking practices. For example, through the ISAC portal, Swift shares relevant information on the Log4j vulnerability and the actions Swift users should undertake. The timeliness and comprehensiveness of the information sharing on such events is also covered by the overseers' review.

4.2.4 ISO 20022 migration

In close cooperation with its user community, Swift has been in the process of developing and testing ISO 20022, a richer and standardised information which is intended to promote greater transparency and speed, and lower cost for cross-border payment transactions. Swift originally planned to initiate the migration phase in November 2022. This launch date has been postponed, due to requests from the user community. At the end of 2022, the European Central Bank announced that it would delay the ISO 20022 migration within the Eurosystem by four months. Upon this announcement, Swift followed a community request to postpone the start of the cross-border ISO 20022 to March 2023 to align the start of the global ISO 20022 migration for CBPR+ with the ECB's updated timetable to ease implementation. This co-existence period, during which users will be expected to switch from the legacy FIN MT to the new ISO 20022 MX format, will thus start in March 2023 and end in November 2025.

Nothing prevents individual users to already exchange ISO 20022 messages sooner than this revised launch date. Since August 2022, all required capabilities have been deployed and institutions have been able to exchange ISO 20022 messages for CBPR+ on an opt-in basis. As such, institutions wanting to realise the benefits of ISO 20022's rich data format for CBPR+ sooner than March 2023 can continue to exchange ISO 20022 messages on an opt-in basis.

As a global standard-setter, Swift takes the lead in coordinating the ISO 20022 migration for its community. From the beginning, overseers have closely monitored Swift's approach, project management and planning, risk assessment, and communication with users. A recent development that Swift announced was the launch of the in-flow translation service, which will be made available for testing before the migration starts, and enables receipt of both FIN MT and ISO 20022 MX messages. With this service, Swift wants to make sure that participants can switch at their own pace during the co-existence period until November 2025. Overseers have closely analysed the scope and testing of the service. On Swift's side, everything has been brought up to readiness to support the global migration of the financial community to ISO 20022 by March 2023.

BOX 10

Impact of sanctions on Swift

The Russian Federation's invasion of Ukraine in February 2022 has had profound and cascading effects on geopolitical relations and the global economy. One of the measures taken in consequence was the European Commission's various sanctions packages targeting entities in or affiliated with Russia or Belarus. Included in these packages is the prohibition to provide specialised financial messaging services to the banks specifically listed in the sanctions decisions. As Swift is under EU and Belgian jurisdiction, in order to remain compliant with European laws and regulations, Swift was required to disconnect those Russian and Belarusian banks from its financial messaging network falling under applicable council regulation.

In order to be continuously in compliance with European laws and regulations, Swift is expected to keep track of changes in the ownership structures of its users, as any legal person, entity or body established in Russia or Belarus whose proprietary rights are directly or indirectly owned for more than 50 % by a sanctioned entity will also become a sanctioned entity by operation of law and should be disconnected from Swift's financial messaging network accordingly.

As pointed out in section 2.1, Swift FIN traffic growth in 2022 was slightly lower than in previous years, in particular for payments. One of the explanatory factors is the traffic lost because of the disconnection of sanctioned banks, next to the reduced interactions with Russia and Belarus triggered by sanctions overall. Year-end figures for 2022 show that Swift FIN traffic sent/received by Russia declined by 56 % and 61 % respectively; for traffic sent to / received from Belarus, the decrease was 50 % and 52 % respectively. This fall in traffic only kicked in as of March/April 2022, following the Russian invasion of Ukraine and the ensuing establishment of sanctions.

4.2.5 Transaction Management Platform

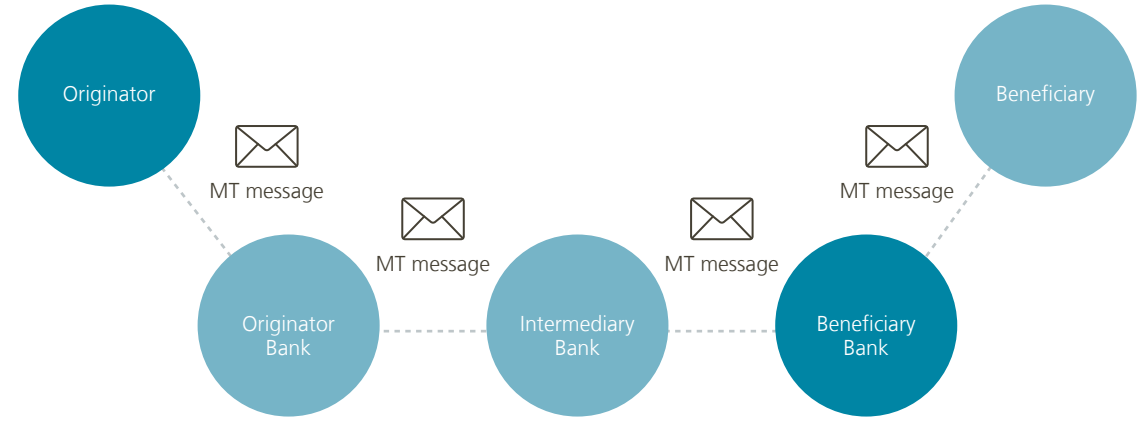
In 2019, Swift revealed their plans to build the Transaction Management Platform (TMP), moving away from traditional sequential messaging to an orchestrator which allows every single participant within a transaction to have an end-to-end and up to date view on the status of the transaction. Swift's Transaction Manager has been deployed live since November but has not yet been processing live customer traffic. Traffic build-up will start from the end of May 2023 until the end of September 2023. The move from FIN MT to ISO 20022 MX is not dependent on the activation of the TMP.

As the following figure illustrates, Swift's current message flow consists of MT messages forwarded from originator to beneficiary using Swift's secure communications channel. Swift's processing is message-driven and there is no central notion of the end-to-end transaction generating the underlying messages between all parties involved.

By evolving from secure message forwarding to end-to-end transaction management orchestrated by TMP, Swift wants to use richer data and reduce friction (i.e. provide better customer experience, increased efficiency, and new value-added services such as transaction validation). The following figure shows that the underlying communication channel for a transaction is format agnostic and could be FIN MT, ISO 20022 MX or Application

Figure

Current sequential Swift message flow

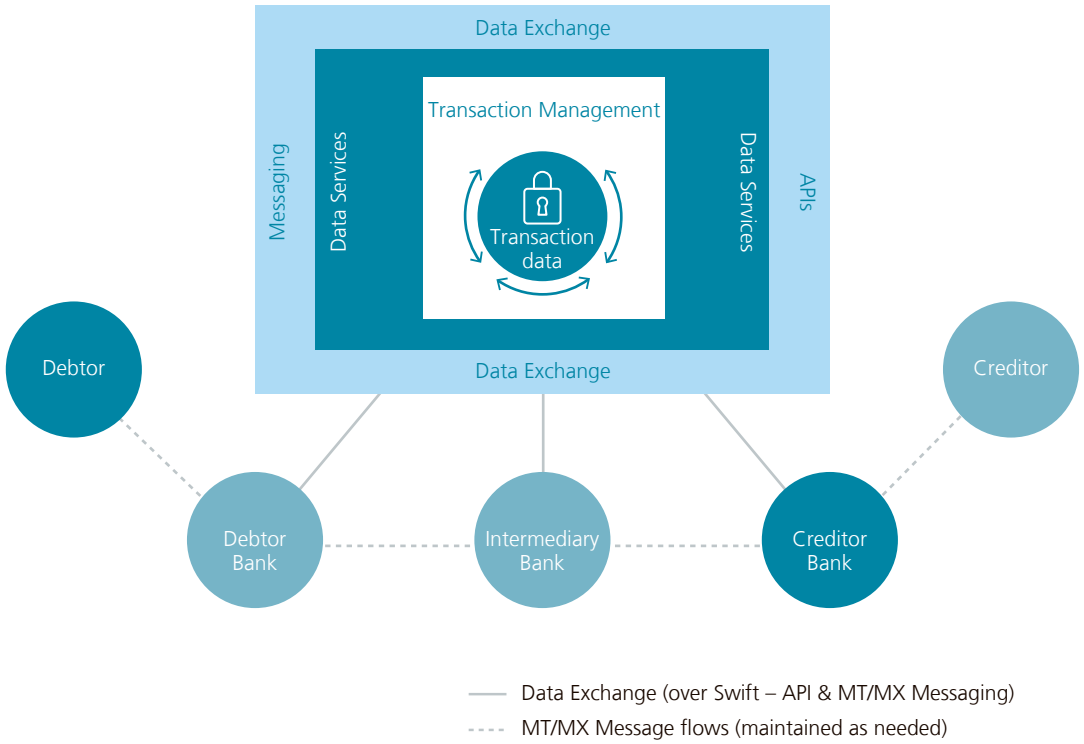


Source: Swift.

Programming Interfaces (APIs), or a combination of channels based on the capabilities of the transaction parties involved (i.e. backward compatibility). The platform maintains full transaction data accessible to any authorised party in the transaction chain, helping to ensure end-to-end transparency. TMP in future could also facilitate the use of APIs so that authorised users can retrieve the transaction status via an API call over the Swift network.

Figure

Planned end-to-end Swift transaction flow



Source: Swift.

TMP has a major impact on Swift's core messaging operations since it changes the payment message flow approach. Therefore, overseers have repeatedly conducted thorough reviews to obtain a complete picture of all relevant HLE aspects of TMP: analysis of risk assessments and corresponding mitigating actions, security and resilience features of the platform, architectural blueprint, project management, customer communication and engagement initiatives. Since TMP touches upon all five HLEs, the project has been part of the continuous oversight monitoring activities. Despite Swift confirming project delivery within the revised timeframe by the end of May, with the first full-scope version forecasted to roll out by September 2023, overseers will continue their critical and risk-based review of the project throughout 2023 and after its launch.

4.2.6 Faster payment initiatives

Launched in 2017, Swift global payments initiative (gpi) has gained momentum as the new standard for cross border, large value payment transactions. Swift gpi combines the traditional Swift messaging and banking system with a new set of rules. Any financial institution joining gpi has to follow these rules, which include transparency of fees, end-to-end payment tracking, and confirmation of credit to the recipient's account. Each transaction is assigned a Unique End-to-End Transaction Reference (UETR) that payment providers can use to trace the transfer from start to finish.

The benefits for customers joining gpi are numerous. First of all, gpi substantially increases payment speed. It eliminates payment friction and reduces the risk of delays through upfront account verification. Another way gpi reduces friction is through automated exception management processes, enabling users to easily handle queries between banks on the Swift network and resolve instances when payment information is incorrect or missing.

Another important dimension from the viewpoint of participants in cross-border transactions is financial crime compliance. Gpi offers a portfolio of financial crime compliance solutions that help member institutions to navigate more complex compliance requirements.

Gpi perfectly fits into Swift's strategy for fast and frictionless messaging services. As the benefits of gpi are realised leveraging the existing Swift messaging infrastructure, users can expect the same level of security and resilience as is the case when using traditional Swift messaging services.

Whereas Swift gpi facilitates high-value or wholesale cross-border payments, Swift Go aims to deliver on the strategy of fast and frictionless payments for low-value international payments. Introduced in July 2021, Swift Go is an interbank service that makes it quicker and cheaper for participating banks to send low value cross-border payments, with the possibility of instant settlement. It enables sending banks to fully customise their front end to offer an easy and intuitive payments experience to their customers. As such, Swift wants to ensure that the traditional banking sector remains competitive in the high-growth market of low-value cross-border payments.

Swift Go uses the Swift gpi rails to deliver speedy cross-border payments. It leverages enhanced service levels between banks, a single payment format and pre-validation services, ultimately removing delays caused by frictions in the transaction chain. In addition to faster payments, Swift Go offers more competitive processing fees, additional transparency, predictability, and payment tracking, combined with the security that users have come to expect from Swift. More than 400 customers have signed up for Swift Go, covering more than 110 countries. Of those, more than 60 banks were live by the end of 2022[1].

Both these services, which are gaining momentum and global reach, demonstrate Swift's continued commitment to delivering on the company's strategy of fast and frictionless payments for its global user community. The products have been repeatedly reviewed by overseers on their functionality, interaction with core messaging services, security aspects, proposed enhancements, and adoption rates.

1 Swift Go: The new standard in low-value international payments, Sibos 2022 in Amsterdam.

BOX 11

Swift's innovations with regard to CBDCs and tokenised assets

As well as trying to solve current challenges on the payments and securities markets, Swift is also looking ahead at the future. With the emergence of innovations such as Central Bank Digital Currencies and tokenized assets, Swift is assessing the role it could play to counteract the potential fragmentation in financial markets caused by these innovations becoming mainstream technologies.

To this end, Swift has set up experiments demonstrating the capability to leverage its existing infrastructure to handle CBDCs and tokenised assets on existing financial infrastructure. This is seen as a major milestone towards enabling their smooth integration into the international financial ecosystem.

At the time of writing, 114 countries, representing over 95 % of global GDP, are exploring a CBDC [1]. They often use different technologies, with primary focus on domestic use. For the potential of CBDCs to be fully realised across borders, these digital currencies need to overcome inherent differences to interact with each other, as well as with traditional fiat currencies.

In collaboration with Capgemini, Swift has made CBDC-to-CBDC transactions between different DLT networks based on popular technologies, as well as fiat-to-CBDC flows between these networks and a real-time gross settlement system. This success showed that the blockchain networks could be interlinked for cross-border payments through a single gateway, and that Swift's new transaction management capabilities could orchestrate all inter-network communication.

Numerous central and commercial banks are collaborating in a testing environment to speed up the path to full-scale deployment.

In a separate experiment with a different group of participants, Swift has similarly demonstrated that its infrastructure can serve as an interconnector between multiple tokenisation platforms and different types of cash payment.

Working in collaboration with many private companies, Swift last year explored 70 scenarios simulating market issuance and secondary market transfers of tokenised bonds, equities and cash. It successfully served as a single access point to various tokenised networks and showed its infrastructure could be used to create, transfer and redeem tokens and update balances between multiple client wallets, as well as providing interoperability between different tokenisation platforms and existing account-based infrastructure.

1 Atlantic Council, Central Bank Digital Currency Tracker, available at https://www.atlanticcouncil.org/cbdctracker.

The World Economic Forum has estimated that the tokenisation market could be worth $ 24 trillion by 2027[1]. Tokenisation has great potential when it comes to strengthening liquidity in markets and increasing access to investment opportunities, and Swift's existing infrastructure can ensure these benefits can be realised at the earliest opportunity, by as many people as possible.

As is the case for the introduction of Swift gpi and Swift Go, these experiments are part of Swift's extensive innovation agenda in support of its strategic focus on enabling instant, frictionless and interoperable cross-border transactions.

1 HSBC, The 10x potential of tokenisation – Democratising investment opportunities, available at https://www.gbm.hsbc.com/-/media/gbm/insights/attachments/potential-of-tokenisation.pdf.

4.3 Focal points for oversight in 2023

The annual planning of Swift oversight is driven by a risk-based approach. The oversight risk assessment helps to maximise the effectiveness and efficiency of the review activities. The assessment of the work in 2022 feeds into the 2023 planning. After each quarter, overseers look into the topics analysed and decide which ones require deeper review, or the items for which Swift needs to provide additional information. This approach creates sufficient flexibility for overseers to dedicate more time to certain topics when needed, or to hold a follow-up discussion at a later stage.

Swift operates in a changing environment with ever fiercer competition and rapidly evolving technologies. That context affects Swift's go-to-market strategy (e.g. agile software development) and operations (e.g. incident management), and poses additional challenges, such as geopolitics, the global scarcity of skilled resources and the changing cyber threat landscape. Overseers are aware of the pace of change and will continue to monitor how it affects Swift in terms of technology planning, resilience guarantees, risk assessments, security decisions and design choices, while keeping users properly informed. At all times, overseers seek assurance that the identified risks arising from new technology choices and major projects are adequately managed and mitigated, to ensure business continuity with comparable or better resilience.

The cyber security strategy and management of risks also remains a major topic on the overseers' agenda for 2023. Overseers analyse which security investment and enhanced capabilities will contribute to Swift's protection against more sophisticated cyber attacks. The cyber security review also involves challenging the ISAE3000 reports conducted by Swift's external security auditor. These reports provide independent assurance on Swift's internal control policies, procedures and controls structured around the five HLEs. The ISAE3000 reports consist of valuable information of importance to the oversight on Swift and are thoroughly reviewed each year.

The follow-up on CSP is also part of the oversight activities for 2023. Overseers will take a closer look at the supervisory involvement and the improvement measures that Swift takes, the CSCF review, the outcome of the first independent assessments, CSP metrics and further refinements, the Swift user community's level of compliance

with the CSCF controls, developments concerning customer cases, results of the new cycle of mandatory independent assessments, and other relevant CSP initiatives and campaigns. In its capacity as lead overseer, the National Bank of Belgium will also hold an outreach session with the Swift Oversight Forum to provide an update on the proposed changes to the CSCF. In doing this, the NBB urges other national authorities to keep pushing their institutions under supervision to improve their endpoint security, as well as for authorities and supervisors to leverage the capabilities of the Know-Your-Supervisor Self-Assessment data within their oversight toolbox.

In 2023, overseers will also aim to get better insight into the broader area of third-party risk management (TPRM) and supply-chain risk management. The distributed and interconnected nature of information technology products and services, and the potential risks that this might pose to financial market infrastructures, has been gaining attention over recent years. Diligent management of exposures to cyber security risks throughout the supply chain and guarding against threats and vulnerabilities among third-party suppliers or their products and services is the main goal of TPRM. This already was a recurrent topic within Swift oversight, but will be given renewed focus during 2023.

Two large projects – TMP and ISO 20022 migration – will reach their delivery deadline in 2023. Overseers have already conducted recurring and thorough reviews of these two projects but will continue to do so during 2023, with stronger focus on the final preparations before launch and communication with customers.

Another area covers major standing topics such as interactions with the risk department and internal audit. Each review cycle includes a dedicated touchpoint with the second and third lines of defence (LoD) to gain a clear understanding of their activities and obtain their views on certain projects and developments at Swift. Following the on-site reviews (OSRs) of the second line of defence (2018) and of the first line of defence (2020), overseers decided to conduct such a review on the third line of defence in 2022. The on-site review resulted in the opinion of overseers that Swift complied with the Institute of Internal Auditors' International Professional Practices Framework (IPPF), which forms authoritative guidance for internal audit professionals worldwide. The results of this review have been shared with Swift, and for those areas where further improvements were suggested by the OSR team, overseers will follow up with Swift throughout 2023 on the status of implementation of these improvements. Another OSR will be performed in 2023, demonstrating the success of this form of collaborative oversight, and leveraging the expertise from other central bank participants to focus on any particular domain for which overseers want to gain additional assurance.

The oversight planning for the following year is structured around the five HLEs which form the starting point for selecting topics for review. Following a risk-based approach, the previous year's assessment forms the basis for the review activities of the coming year. For 2023, this resulted in an extensive set of topics to be analysed by overseers, of which the following are a sub-set:

- HLE 1 Risk Identification and Management
  - Operational impact of the pandemic;
  - Internal and external audit findings;
- HLE 2 Information Security
  - Cybersecurity roadmap;
  - Customer incidents and forensic capabilities;
- HLE 3 Reliability and Resilience
  - Business continuity exercises;
  - Impact of technological developments on Swift's resilience;
- HLE 4 Technology Planning
  - Financial Crime Compliance portfolio;
  - Transaction Management Platform & ISO 20022 migration;
- HLE 5 Communication with Users
  - Customer communication related to ISO 20022 migration;
  - Customer adoption plans.

Specific thematic articles

5. Specific thematic article: 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 covers some of the cyber- and ICT-related threats and risks faced by financial institutions in general, as well as by financial market infrastructures, payment institutions and electronic money institutions in particular. This description is followed by a summary of the various initiatives, taken by the Bank in this context, both on the regulatory and supervisory side. Finally, there is an overview of common observations made during on-site inspections focused on cyber and ICT risk, again paying particular attention to FMIs, PIs and ELMIs.

Continuing rise in cyber and ICT threats

2022 was still marked to some extent by the after-effects of the COVID-19 pandemic. However, the associated challenges, such as mass working from home, more limited physical presence of operators, specific attack patterns, etc. were mostly adequately dealt with in the financial sector. The solutions found are now often part of the "new normal".

In February 2022, the geopolitical conflict in Eastern Europe took an important turn with Russia's invasion of Ukraine. Given the broad and explicit Western support for Ukraine and the European sanctions against Russia, it suddenly became much more likely that European countries, and in particular Belgium given the presence of several international institutions, would become the target of cyber attacks committed by either groups linked to nation states, or so-called "hacktivists". Scenarios in which the attackers unintentionally cause collateral damage should also not be ruled out, as well as attacks on non-financial critical infrastructures (telecom, energy, etc.), which could have a substantial impact on the financial sector. The Bank and the entire financial services industry have been in a heightened state of preparedness since the escalation of the conflict. Fortunately, thanks to various precautionary measures, this concrete threat did not lead to any major operational incidents during the reporting year.

In any case, cyber attacks have evolved worldwide into an everyday reality in recent years. Malicious actors are further honing their techniques and methods, resulting in some of the attacks becoming increasingly sophisticated, powerful and/or enabling large-scale campaigns. The number of persistent and targeted cyber attacks is therefore expected to rise further in the future, with the financial sector most probably remaining a potential high-value target. Cyber attacks may result in the theft of sensitive data, system disruption, initiation of fraudulent transactions, etc. This often involves the use of ransomware, distributed denial-of-service (DDoS) attacks, abuse of credulous employees or exploiting other vulnerabilities in the infrastructure and processes of institutions, including their supply chain. See box 1 for a detailed and more technical description of recent developments in cyber threats.

Apart from cyber risks, the financial sector's heavy dependence on IT solutions also throws up other challenges. Under pressure from innovative players and higher customer expectations regarding services offered, traditional institutions are forced to renew their at times outdated IT architecture in a relatively short timeframe. Growing security concerns, triggered for example by the use of "end-of-life" software that the vendor no longer supports, only add to this sense of urgency. However, the complexity of these institutions' IT environments makes their responsible modernisation a major challenge in some cases. 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 a growing number of critical processes. That is also one of the reasons why, across the sector, a small number of critical service providers present an ever-increasing concentration risk for the financial industry. In recent years, it has also become very clear what impact geopolitical tensions can have on certain supply chains. The need for sufficiently representative testing of developed software and recovery solutions for various extreme but plausible scenarios remains another key point of attention.

In order to monitor and keep the risks within appetite, it is important for financial institutions' management bodies to acquire the necessary information and intelligence (on external threats and the institution's operational resilience), to have appropriate expertise available, and to incorporate adequate countermeasures in the strategic planning. But quite a few institutions admit they have difficulty in recruiting sufficient staff with the required cyber/ICT expert skills.

Regulatory and legislative developments

In recent years, the Bank has made a substantial contribution to the development of a regulatory framework to improve 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 has also made an active contribution to establishing a European regulatory framework for the management of cyber and ICT risks. Under the aegis of the EBA, this resulted in the publication of a set 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 all become part of the Bank's supervision and policy framework. For payment systems and market infrastructures, the ECB's oversight expectations regarding cyber resilience are providing guidance[5]. Last but not least, there have also been important developments at global level: in March 2021, the Basel Committee on Banking Supervision published new principles for strengthening the operational resilience of banks, including specific focus on ICT and cyber security[6].

On 17 January 2023, the Digital Operational Resilience Act (DORA) entered into force. This EU regulation aims to mitigate the risks associated with the digital transformation of the financial industry by imposing strict and common rules on ICT governance and risk management, ICT incident reporting and information-sharing, security testing and ICT third-party risk. These rules will apply to a wide range of financial institutions, as well as critical ICT third-party service providers, for example cloud service providers, that will be subject to a form of EU oversight. During negotiations on the draft texts at European level, the Bank played an important advisory role in the Belgian delegation. In the meantime, NBB experts are intensively involved in the development of technical standards that will further underpin the DORA Regulation. More information on this topic can be found in box 12.

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).
5 ECB Cyber resilience oversight expectations (December 2018).
6 BCBS Principles for Operational Resilience (March 2021).

BOX 12

Digital Operational Resilience Act

On 17 January 2023, the EU Digital Operational Resilience Act (DORA) entered into force[1] after more than two years of negotiations. Its provisions will apply as of 17 January 2025. The initiative came from the European Commission's Directorate-General for Financial Stability, Financial Services and Capital Markets Union (DG FISMA) in response to the 2019 joint technical advice from the European Supervisory Authorities (ESAs) that called for a more coherent approach in addressing ICT risk in finance[2] and as part of a much broader Digital Financial Strategy setting out broad guidelines on how the European Union intends to support the digital transformation of finance in the coming years, while regulating and mitigating the risks arising from it.

The DORA Regulation is motivated by the ever-increasing dependency of the financial sector on digital assets and processes, resulting in information and 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 on the grounds that current legislation across Member States does not fully address the topic in a detailed and comprehensive way, does not provide financial supervisors with the most adequate tools to fulfil their mandates, and leaves too much room for diverging approaches across the Single Market.

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 other things, the crucial and active role the management body has been in steering the ICT risk management framework. 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, besides 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 goal is for financial entities to have to 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. In the same spirit, the incident reporting obligations under PSD2 will be fully integrated into this new incident reporting framework.
- The third pillar addresses requirements for **digital operational resilience testing**, i.e. periodically assessing cyber resilience 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

1 Regulation (EU) 2022/2554 of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No. 1060/2009, (EU) No. 648/2012, (EU) No. 600/2014, (EU) No. 909/2014 and (EU) 2016/1011 (14 December 2022)

2 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).

making use of tests ranging from vulnerability scanning to software code analysis, only those entities identified by competent authorities as significant would be required to conduct advanced threat-led penetration tests.

- Fourth, the proposal contains provisions to 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 that harmonises 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 a Union oversight framework**.
- The last and fifth pillar raises awareness around ICT risk and related aspects such as: minimising the propagation of risk, supporting financial entities' defensive capabilities and threat detection techniques, explicitly allowing financial entities to set up **cyber threat information and intelligence exchange** arrangements amongst themselves.

A broad range of financial entity types falls under the scope of DORA, including central securities depositories, credit institutions, insurance and reinsurance undertakings, investment firms, payment institutions and 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 and more stable overall financial system. Operators of payment systems and entities involved in payment processing remain out of its scope for the time being.

DORA is to be considered *lex specialis* with respect to the EU Directive on measures for a high common level of cyber security across the EU (also referred to as the NIS 2 Directive)[1]. This means that the requirements under DORA regarding for example ICT risk management and ICT-related incident reporting are in principle more far-reaching than those under the NIS 2 Directive and that institutions in the personal scope of the Regulation only have to comply with the DORA provisions, unless the national transposition of NIS 2 would explicitly extend the scope or provisions of the NIS 2 Directive (and therefore deviate from the minimum harmonisation principle).

The EU legislators have further specified that, given the strong interlinkages between the digital resilience and the physical resilience of financial entities, the obligations laid down in Chapters III and IV of the Directive on the resilience of critical entities (CER)[2] should not apply to financial entities falling within the scope of DORA. Here too, the national transposition of CER could still extend the scope or provisions of the CER Directive.

Overall, the National Bank of Belgium is very supportive of the DORA initiative, its ambition to strengthen digital operational resilience and to further harmonise ICT risk management practices and requirements in the financial sector. It is fully committed to a successful implementation of DORA and is actively contributing to the establishment of level-2 texts that will support the final DORA Regulation.

1 Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No. 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (14 December 2022).

2 Directive (EU) 2022/2557 of the European Parliament and of the Council on the resilience of critical entities and repealing Council Directive 2008/114/EC (14 December 2022).

Finally, in early 2022, the European Systemic Risk Board published recommendations for the establishment of a pan-European framework for coordinating cyber incidents of a systemic nature. The Bank is also closely involved in the elaboration of these recommendations.

Supervisory activities

The traditional supervisory 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 the IT systems and data are crucial here. As in recent years, the Bank conducted a number of inspections in 2022 to check compliance with the regulatory framework and to verify the proper management of IT systems in relation to cyber and ICT risks (see also next section).

In addition, the Bank monitors these risks in financial institutions and FMIs during its ongoing and recurrent supervisory activities. In March 2022, in response to the heightened cyber threat posed by the Russian invasion of Ukraine, the Bank decided to raise awareness among the institutions under its supervision on the cyber threat posed by this crisis and to urge them to improve their operational preparedness. In addition, a selection of significant institutions was requested to complete a short survey. The answers to this survey were further supplemented during follow-up sessions with the respondents. After a thorough analysis of the various responses, the Bank can conclude that the sector was generally well aware of the heightened threat level and that it responded appropriately.

The Bank is also taking other sector-wide initiatives. Inspired by the approach for credit institutions under the SREP, some FMIs, payment institutions and electronic money institutions are requested to respond to IT risk questionnaires on a regular basis. This provides important data for the prioritisation of supervisory work and also permits cross-sectoral analyses. One novelty this year was that a selection of financial institutions was asked to provide a list of the arrangements they have with ICT third-party service providers. This exercise was part of an initiative of the European Supervisory Authorities (ESAs), which in this way tried to obtain a first view of the third parties that could in the future be designated as critical service providers under the DORA Regulation.

In 2018, the Bank set up a framework for ethical hacking, namely TIBER-BE (Threat-Intelligence- Based Ethical Red Teaming Belgium). This program is the Belgian implementation of a methodology developed by the Eurosystem, which aims at increasing the cyber resilience of individual FMIs and financial institutions through sophisticated tests, as well as to gain important insights into the cybersecurity of the Belgian financial sector as a whole. The Bank encourages these exercises in its role as catalyst for financial stability. More information on this TIBER-BE implementation can be found in the thematic article 8 on TIBER-BE.

In its role as the sectoral authority for 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 infrastructure. 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.

The Bank also takes part in various international working groups and forums to gain a better understanding of the risks that could become systemic for the financial sector and to study mitigating measures. Other initiatives aim to promote the exchange of information between institutions, supervisors, central banks, etc.

Common observations from on-site inspections

As mentioned previously, a number of FMIs, PIs and ELMIs were subject in recent years to on-site inspections focused on cyber and ICT risks. These activities frequently resulted in similar observations. Below is an overview of some of these thematic findings:

- In many cases, institutions still need to make 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 comprehensive reporting on these risks and their evolution associated with the implementation of mitigating measures and related 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, treatment, monitoring and reporting of all identified risks.
- In a number of cases, institutions were found to have insufficient resources or expertise, or not to operate efficiently enough to manage and 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 more regularly organise initiatives to make their staff aware of security risks and monitor the effectiveness of these initiatives. These 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 infrastructure 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. And, as mentioned earlier, it is crucial that institutions proactively identify which software is nearing the end of its life cycle and take timely measures 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, including so-called intra-group arrangements, 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 sufficiently monitored and regularly audited.
- Another recurring topic 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 (i.e. multi-factor) 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. often remain 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 plans more regularly and do this 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 resulting findings and recommendations are addressed as soon as possible.

6. Specific thematic article: Targeted Supervision further maturing in 2023 with a proper assessment of restitution risk

Dorien De Beuckeleer and Ingmar Vansieleghem

Custodian banks are licensed as credit institutions under Article 4(1) of the Capital Requirements Regulation as they collect deposits from their clients and grant (mostly intraday) credit for operational purposes. Yet, they offer far fewer traditional banking services like loan origination or maturity transformation. Instead, as their name implies, custodians hold and service assets under custody from their clients. This specific business model brings its own risk profile. Despite the differences, custodian banks are subject to same prudential requirements as all other licensed credit institutions under the CRD/CRR. The SSM will accordingly monitor compliance with these requirements, with the objective of ensuring equal treatment of all supervised institutions in a level playing field perspective.

However, making sure of this level playing field and equal treatment of all supervised institutions, requires not only a standardised methodology to be applied, but also account to be taken of the specific risks an institution may face owing to their specific business model or environment. The Bank has accordingly raised awareness and contributed to developing a specific methodology to assess restitution risk within the relevant SSM working groups.

Restitution risk was introduced by the Alternative Investment Fund Managers Directive (AIFMD) and the Undertakings for Collective Investments in Transferable Securities Directive (UCITS)[1]. These Directives, dating from more than a decade ago, both introduce the so-called restitution liability. Depositories are liable to fund any loss of financial instruments held in custody. Delegation of the safeguarding duties to a third party has no impact on the liability unless certain conditions have been met or when a contract expressly transfers the liability. Legislation also further clarifies that credit institutions are not liable in all circumstances. The depositories are not liable when they can prove that the loss has arisen as a result of an external event beyond reasonable control, the consequences of which would have been unavoidable despite all reasonable efforts.

The Directives set out precisely all aspects related to the liability, such as when a loss is deemed to have taken place and how such a loss shall be ascertained by the fund manager. Also, more precise definitions of what constitutes *external events* and what triggers an event to be *beyond reasonable control* are provided.

Custodian banks safeguard the lion's share of all assets held under custody, yet not all of them. So, they are not the only credit institutions to which these Directives apply. Among other credit institutions impacted by this legislation are some of the larger European universal banks. Also, depositories are not liable to 'restitute' all

1 These Directives set out a clear framework for the regulation and supervision of European fund classes and thus ensure greater investor protection.

assets they hold in custody. Only those assets, or more precisely funds, that are subject to the AIFMD and UCITS have to be compensated when lost.

The CRR, the Regulation defining the scope and methodology for determining the capital requirements for all licensed credit institutions, currently does not cover restitution risk and does not provide any methodology to determine the corresponding capital charge. So, credit institutions often cannot prove that they hold (adequate) capital to cover their exposure to restitution risk.

In 2022, the National Bank helped the SSM raise awareness of restitution risk within the appropriate working groups. By 2023, all credit institutions will have been advised to consider that risk – wherever relevant – in their internal capital requirement calculations. Based on these calculations, a dedicated horizontal assessment of the risk should be carried out for the first time in 2023. Targeted supervision, which enables JSTs to better focus on those risks which contribute to credit institutions' risk profiles is further maturing this year.

7. Specific thematic article: Environmental and climate-related risks within the FMI landscape

Dorien De Beuckeleer

As climate and environmental risks are becoming increasingly important and are gaining attention in the financial sector, the NBB has also started to pay more attention to these risks within the scope of financial market infrastructures, custodian banks, payment transaction processors and messaging services landscape. So, at the end of 2021 and early 2022, it asked a sample of Belgian institutions active in this area to complete a questionnaire on climate and environmental risks (hereafter, the NBB questionnaire). The first findings from this survey were set out in the 2022 NBB Financial Market Infrastructures Report.

Some institutions that also have a banking licence were also requested in 2021 and/or 2022 to fill in a new questionnaire under banking supervision regulations. If the bank was a significant institution[1], the questionnaire was set up and reviewed at the level of the Joint Supervisory Team (JST)[2], whereas this exercise was coordinated by the NBB for Belgian less significant institutions[3]. The main building blocks of the different questionnaires (NBB and ECB) generally covered the same topics, namely materiality, business model, governance, risk appetite and management.

Over the course of the year 2022, the NBB, along with the JST for significant banks, held several follow-up interactions on climate and environmental risks with a representative sample of the institutions covered by this article. These meetings had different objectives, e.g. dialogue regarding the reviews from the 2022 survey carried out by the supervisory teams, discussion of actions taken and presentation of corporate action plans for climate and environmental risks.

More and more market and supervisory authorities, policymakers, and other stakeholders are publishing guidance and frameworks about climate and environmental risks. These frameworks and good practices include:

- Task Force on Climate-related Financial Disclosures (TFCD); Recommendations of the Task Force on Climate-related Financial Disclosures[4].
- BCBS Principles for effective management and supervision of climate-related financial risks[5].

1 Banks under direct supervision of the single supervisory sechanism (SSM).
2 For more information, see direct versus indirect supervision: https://www.bankingsupervision.europa.eu/banking/list/html/index.en.html.
3 Banks under direct supervision of the national competent authority.
4 Available at https://www.fsb-tcfd.org/recommendations/.
5 Available at https://www.bis.org/bcbs/publ/d532.htm.

- Climate Financial Risk Forum[1]: 2020 Guide to help the financial industry approach and address climate-related financial risks[2].

- Climate Financial Risk Forum: Second set of guides to help the financial industry effectively manage climate-related financial risks (2021)[3].

- ECB guide on climate-related and environmental risks: supervisory expectations relating to risk management and disclosure[4].

- ECB: Good practices for climate-related and environmental risk management: observations from the 2022 thematic review[5].

- EBA: Final draft implementing technical standards on prudential disclosures on ESG risks in accordance with Article 449a CRR[6].

- Best Practices for Sustainability Reporting: NYSE ESG Guidance[7].

- Various guidance from the European Commission on sustainability disclosures[8].

This is a non-exhaustive list of frameworks, as supervisory authorities, policymakers and other stakeholders continuously develop and refine their frameworks, guidance and best practices. The best practices put forward in this article come from a combination of requirements and best practices as defined in the different frameworks. According to each institution's specific legal status and licence, one or more of these frameworks can refer to institutions covered by this article. Institutions within the scope of financial market infrastructures (FMI), custodian banks, payment transaction processors and messaging service providers are advised to apply the applicable frameworks. If there is no specific framework for their type of institution, they are advised to apply the most relevant best practices and recommendations.

As already mentioned, some of the institutions targeted in this article that also hold a banking licence have already been asked to comply with several of these guidelines under banking supervision regulations, such as the ECB guide on climate-related and environmental risks that lists supervisory expectations relating to risk management and disclosure[9]. The NBB approach to climate and environmental risks encompasses the entire FMI, custodian and payment transaction processors and messaging services landscape whatever their status and related set of applicable guidelines, as well as their relative maturity and implementation timeline.

Continued interaction with and analysis of climate and environment-related topics will include firm-specific analysis as well as horizontal reviews. The firm-specific analysis can point up strengths and weaknesses, opportunities and threats, as well as progress made by the institution itself. The horizontal reviews include such

1 A UK forum on climate risks bringing together senior financial sector representatives (e.g. asset managers, banks, insurers, London Stock Exchange group) to share their experience in managing climate risks; co-chaired by the PRA and FCA (website: https://www.fca.org.uk/transparency/climate-financial-risk-forum).

2 Available at https://www.fca.org.uk/publication/corporate/climate-financial-risk-forum-guide-2020-summary.pdf.

3 Available at https://www.bankofengland.co.uk/news/2021/october/climate-financial-risk-forum-session-two-outputs.

4 Available at https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.202011finalguideonclimate-relatedandenvironmentalrisks~58213f6564.en.pdf.

5 Available at https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.thematicreviewcercompendiumgoodpractices112022~b474fb8ed0.en.pdf.

6 Available at https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Draft_Technical_Standards/2022/1026171/EBA_draft_ITS_on_Pillar_3_disclosures_on_ESG_risks.pdf.

7 Available at https://www.nyse.com/esg-guidance.

8 Available at https://finance.ec.europa.eu/sustainable-finance/disclosures/corporate-disclosure-climate-related-information_en.

9 Available at https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.202011finalguideonclimate-relatedandenvironmentalrisks~58213f6564.en.pdf.

things as descriptions of general trends and developments observed (e.g. the climate and environmental domains in which the most progress was made and which domains are still in the early development stage) within the FMI landscape, custodian banks, payment transaction processors and messaging service providers, as well as highlighting similarities and differences noted between different institutions. More broadly speaking, these analyses can give an indication which institutions are making the most progress and which ones are lagging behind their peers on the different climate and environmental dimensions of the framework, thus giving a robust base for benchmarking and a level-playing- field setting.

Follow-up work consists of a mix of global reviews as well as in-depth analysis of selected domains impacted by climate and environment-related risks and opportunities. Information providing input for the analysis has been collected from different sources. At the end of 2021 / beginning of 2022, institutions were asked to fill in a new questionnaire on several climate and environment-related topics. Underlying documentation provided by the institutions will be analysed by the supervisory/oversight teams. Public disclosures will also be reviewed. Further meetings with the institutions will be organised to discuss the actions they have taken and any future actions plans, any information provided as well as the outcome of the analysis.

The NBB will focus on the following domains which will be impacted by climate and environmental risks when it comes to identification, management and public disclosure of climate and environmental risks.

I. Materiality, business model and environment

To ensure the sustainability as well as the resilience of their business model in the short-medium to long term, financial institutions should regularly assess the materiality and the current and forward-looking impact of potential business and risk drivers. Follow-up to the materiality assessment and business model impact includes topics like assessments carried out by the institutions, processes put in place to perform the analysis, the impact on the institutions' business model, strategy and product offering and the role institutions believe they can play within the financial sector with regard to climate and environmental risks.

The results of the NBB questionnaire have shown that some of these institutions had already carried out a preliminary qualitative assessment of the residual exposures to climate risk in the short and medium term and have taken steps to identify and measure climate and environment-related risks, but further progress on this topic is required.

As climate and environmental risks can impact different aspects of the institutions – ranging from new and greater risks, pressure on profitability, to changes to the business environment in which they operate, their competitive position and product offering – it is critically important that institutions (continue to) assess the materiality of climate and environmental risks in the short, medium and long term. They should identify which climate and environmental elements are the most important for them, any potential threats for their future business and the opportunities they could put forward. This information should enable the institution to make well-informed decisions about business strategy, risk management and regulatory compliance based on a comprehensive set of elements (including climate and environmental risks and opportunities).

Both transition[1] and physical[2] risk drivers will affect institutions' potential exposure against climate and environmental risks. The magnitude of both risk type drivers depends on multiple factors, like the type of services offered to clients, the size and timing of mitigation measures, the way the transition occurs (in an orderly or disorderly fashion). Financial market infrastructures, custodian banks, payment transaction processors and

1 Transition risk: Risk inherent in changes related to the process of adjustment aimed at reducing reliance on carbon (low-carbon economy) and its impact on climate. Risks caused by climate-related changes such as changes in public policies and legislation, technology, market and customer sentiment.

2 Physical risks: for instance, economic costs and financial losses resulting from the increasing severity and frequency of climate change-related or extreme weather events, longer-term gradual shifts in the climate, and indirect effects of climate change such as loss of ecosystem services.

messaging services are largely operation-driven institutions, implying that physical risks could heavily impact the provision of services, such as service disruptions due to IT outages resulting from floods and power cuts. This expectation was actually confirmed by the findings from the NBB questionnaire which showed that all institutions identified physical risks, such as extreme weather events and natural disasters, as an important climate and environmental risk category. However, they also listed several transition risk drivers, like higher carbon pricing and energy costs, regulatory uncertainty and legal and compliance risk caused by regulatory expectations about climate risk. Moreover, institutions can be indirectly exposed to the climate risk of their clients, service providers, sub-custodians, their cash correspondents where part of the client deposits are placed and the issuers of the securities in which some of the client deposits are also invested, deterioration in the value of the collateral put up by the clients as well as the assets under custody e.g. if these securities are issued by companies active in "brown[1]" industries or located in countries which are geographically more exposed to climate risks.

Against this background, institutions need to be able to deal with the potential impact of future physical and transition risks on their operational processes, as any disruption of services can result in direct as well as indirect losses that are due to the lost business caused for example by the reputational impact of not being able to deal with the climate and environmental risks.

Besides the impact on the operational processes, it is important for institutions to understand and identify the main issues caused by climate and environmental risks that could impact their business model in the short, medium and long term, so as to be able to take this into consideration in their strategic planning and business decisions (such as the products and services they provide in the short to medium term or develop in the longer term) to preserve their profit-generating capacity. Institutions covered in the NBB questionnaire said they could also play a role in the financial community with regard to tackling environmental and climate-related risks. Public disclosures of different institutions show that the institutions covered by this article are taking action to integrate ESG components into their product/service offering. To give some examples, Swift disclosed in its United Nations Global Compact Progress Report 2021 that it has integrated the International Chamber of Commerce's Sustainable Trade Finance Guidelines into its Know Your Customer Registry platform[2]. Euroclear has announced that it has a partnership with Greenomy, an institution which helps corporates, credit institutions and asset managers to comply with new European Union sustainable finance legislation by digitalising the data capturing and reporting process and providing data analytics features[3]. BNYM group mentioned in its 2021 ESG report that it is now offering clients the option of incorporating ESG factors into collateral negotiations and decisions with their counterparties[4].

The future course of climate change (speed of change, the way changes materialise), as well as the response of different parties (policymakers, competitors, clients) in the long term, is still uncertain. As a result, the materiality assessment conducted by institutions should be repeated on a regular basis and should consider various scenarios. The materiality review is expected to be tailored to the risk profile and the institution's business model and (long-term) strategy. Further, the analysis should consider the business environment (physical locations, counterparties within the value chain, competition, economic and political environment, etc.) in which it operates.

II. Governance, risk management and compliance

A second area of attention is the way the institutions monitor and deal with climate and environmental risks. This contains several sub-elements pertaining to governance, risk management frameworks and compliance with current and future regulation, guidance and standards.

1 Brown industries: industries that perform environmentally harmful activities, amongst others more carbon-intensive economies contributing to the climate change through the emission of greenhouse gases.

2 Available at https://www.swift.com/about-us/discover-swift/corporate-social-responsibility.

3 Available at https://www.euroclear.com/innovation/en/greenomy.html.

4 Available at https://www.bnymellon.com/content/dam/bnymellon/documents/pdf/2021-enterprise-esg-report.pdf.coredownload.pdf.

A first element is how institutions deal with these risks from a governance perspective. This review includes such things as the way the different management levels (executive committee, board and its committees) are kept informed and how they act upon relevant climate and environmental information, and also take into account this information in setting the risk appetite and business strategy of the firm. Further, the integration of these risk drivers within the three lines of defence (business level, risk management and internal audit) could be looked at. Not only should the operational level and risk management consider climate and environmental risks, but internal audit should also assess the adequacy of these institutions' management of climate and environmental risks.

It is important that boards of directors and executive committees are aware of the impact of climate and environment-related risks at the level of the company and the broader business ecosystem (suppliers, clients, stakeholders) and take this into account in their management decisions. The management body should be able to take timely corrective actions if necessary. As a result, adequate reporting throughout the institution and ongoing communication through the various functions is necessary and expected to be set up. The institution should ensure that sufficient expertise is available throughout the company, from operational and business level up to board level and that specific responsibilities are assigned within the organisation's different layers of power. The method of integrating ESG responsibilities into institutions can take different forms. While some may choose to add this new field of competence to their existing structures, others may opt to set up dedicated structures and committees to tackle and coordinate climate and environmental topics. The functions responsible for climate and environmental topics should in any event be given sufficient (financial and human) resources.

A second element concerns the risk management framework. Potential areas of interest in this regard are the existence of processes to identify, measure, mitigate and report on climate and environmental risks throughout the different layers of the institution, inclusion of any identified risks in the risk appetite (both quantitative and qualitative statements), availability of relevant data, incorporation of these risks into stress testing, scenario analysis and business continuity planning.

Climate risk can be considered as a separate risk or as a driver for different risk types. In the latter case, climate risks are mapped to the 'traditional' risk categories, such as operational, credit, market and reputational risk, and are considered as one or more of the elements that can materially impact the size of these 'traditional' risks. In both cases, institutions should include climate risk explicitly in their risk appetite, define risk limits and metrics to monitor changes in climate and environmental risks and implement mitigating measures. The magnitude of the different risk drivers will also depend on geographical location (e.g. floods, heat waves) and macroeconomic developments (e.g. energy prices).

Physical risk drivers as well as transition risk drivers need to be included in the risk appetite. Several institutions pointed out in the NBB questionnaire that they were in the process of defining a statement on their climate-related risk appetite. Adequate metrics need to be developed to monitor these risks to allow timely implementation of mitigating measures and response towards climate-related evolutions and to monitor whether they are on the right path towards meeting the climate and environmental goals set by the institution. Based on the NBB questionnaire, it was concluded that there is still wide room for improvements on internal metrics on climate and environment-related risks. The appropriateness of these internal processes and metrics are expected to be reviewed on a regular basis, taking into account current and future expected developments.

The availability of data and data aggregation capacities are crucial to provide accurate reporting. As several institutions are in the early stage of monitoring climate and environmental risks, the availability of relevant data (internal and external) could be a challenge. To ensure accurate monitoring, institutions should investigate which data they need and which data they are currently lacking.

The magnitude and probability of materialisation of climate and environmental risks should also be considered when institutions draft their business continuity plans. Stress tests and scenario analysis have to include scenarios about climate and environmental risk drivers. Several institutions have already pointed out in the NBB questionnaire that climate-change-related risk drivers are part of their stress testing or extreme risk scenario

analysis. The business continuity plan should also take into account the estimated impact of these risks on the institution's service providers and outsourcing counterparties.

A third element is the compliance with relevant regulatory standards and regulation. As climate and environmental risks are gaining much more attention, supervisors, supervisory agencies and governments are developing new regulations to limit the climate risk impact and are issuing a minimum set of standards institutions are expected to comply with. Institutions should assess the potential impact of regulatory or legal changes on themselves and on their business environment. As a result, institutions need to remain informed about new regulations and guidance. The NBB questionnaire showed up two main challenges. A first challenge to deal with is the higher regulatory expectations. A second challenge is the need to improve data management to identify the right focus.

III. Public disclosures on climate and environmental risks

A third building block in the climate and environmental reviews by the regulators is the institution's public disclosure. This involves several elements, like the type of disclosed information (information on governance, materiality assessment and risk drivers, risk management and appetite, goals etc. for climate and environmental risks), the relevance and accuracy of the published information.

Disclosures on climate and environment-related risks enable market participants to make better informed analysis on the size of these risks facing the different players within the financial sector. Besides the need to develop adequate internal reporting, institutions should also publish sufficiently detailed and accurate, non-confidential information to the public. Different stakeholders (like future employees, suppliers, clients, etc.) will use this information for multiple purposes (e.g. is the institution sufficiently mitigating climate risks to make use of the services offered by the institution, more and more people are considering the impact of the institution on the environment when deciding which firms they want to work for). The NBB questionnaire findings showed that several institutions believe that tackling climate change and actively engaging to improve sustainability will be essential to maintain and strengthen their brand reputation and will also be necessary to meet expectations of clients in the short to long term. One of the institutions even mentioned that it believes proper communication about its climate and environmental measures will be crucial to attract employees in the future. Although action to mitigate climate and environment-related risks positively impact the institution's image and limit its liability risks, institutions should ensure that they do not fall into the trap of "greenwashing" by publishing misleading information which makes stakeholders believe that the company is doing more than it actually is in reality.

Based on the different existing guidance and published best practices, institutions are advised to disclose different types of information to give stakeholders a comprehensive view on the institutions' exposure and mitigating measures with regard to climate and environmental risks. The institutions should share the outcome of the materiality assessment, describe which assessment methodologies they have used, explain why they deem certain climate risk drivers as irrelevant, provide information on the management and governance process relating to these risks, discuss the actions they have taken to mitigate the impact of these risk drivers on the business and risk profile of the institution, publish relevant key metrics on climate and environment-related risks and describe the future goals as well as the current achievements. This will ensure that a comprehensive set of information is available and help stakeholders to draw conclusions and engage with the institution on a well-informed basis. In their public disclosures, institutions are urged to use both qualitative as well as quantitative information.

Policymakers, supervisors and international organisations welcome the sustainability disclosures of financial players and have published guidance on the disclosure of climate and environmental risks in order to limit potential greenwashing and enhance comparability of the institution's reporting. The following paragraphs give a set of examples.

The task force on climate-related financial disclosures, set up by the Financial Stability Board (FSB), has published a report with recommendations on climate-financial related disclosures which are considered to be widely

applicable to organisations across (financial and non-financial) sectors and jurisdictions. These recommendations are structured around four areas, namely governance, strategy, risk management and metrics & targets[1].

For those institutions that also have a banking licence, the ECB/SSM and EBA have published guidance on the public disclosure of climate and environmental risks[2].

The European Union has also defined a set of disclosure requirements on sustainability matters for certain institution types, like large listed companies. At the end of 2022, the EU Council of Ministers gave its final stamp of approval to a new Corporate Sustainability Reporting Directive (CSRD)[3], which will extend the list of institutions in scope. CSRD will apply to all large companies (listed and unlisted), as well as listed SMEs. The extended scope of the CSRD will also affect several institutions covered by this article, as some of these institutions were not yet obliged to report but will now be in scope of the new reporting Directive. The exact scope of the institutions covered across the different sectors will be determined based on an analysis of the Directive. This Directive entered into force as of 5 January 2023. The application date will depend on the institution type (size, listed, etc.). The CSRD will require institutions to have a third-party audit of the publicly disclosed information.

1 Availiable at https://www.fsb-tcfd.org/recommendations/.

2 ECB: available at https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.202011finalguideonclimate-relatedandenvironmentalrisks~58213f6564.en.pdf. EBA: available at https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Draft Technical Standards/2022/1026171/EBA draft ITS on Pillar 3 disclosures on ESG risks.pdf.

3 Availiable at https://finance.ec.europa.eu/capital-markets-union-and-financial-markets/company-reporting-and-auditing/company-reporting/corporate-sustainability-reporting_en.

8. Specific thematic article: Threat-Intelligence-Based Ethical Red Teaming in Belgium (TIBER-BE)

Tijl Jooris

With a high degree of technological progress and growing reliance on related IT infrastructure, cyber risks to the Belgian financial sector are becoming ever more prevalent. One of the NBB's tasks is to monitor Belgian critical market infrastructures and core financial institutions to ensure these key financial entities remain resilient to cyber attacks as to avoid a systemic impact on the Belgian (and by extension European) financial system. To help achieve this goal, the NBB adopted the TIBER-EU Framework in May 2018 and leads implementation of the Threat-Intelligence-Based Ethical Red Teaming framework in Belgium: TIBER-BE.

Since the inception of the TIBER-BE programme, the cyber-threat landscape has changed at a breakneck pace, not least related to geopolitical developments. Besides increased threats from organised criminal groups orchestrating cyber campaigns in pursuit of profit through data theft and ransomware, the Russian invasion of Ukraine has sparked a major uptake in cyber activity by threat actor groups and individuals taking a side in the conflict and conducting operations to support it. For now, related cyber attacks are primarily targeted on Ukrainian and Russian IT infrastructure, but it is not unlikely that stakeholders active in the conflict will eventually shift their focus to targeting nations and entities outside Ukraine and Russia using their newly acquired techniques. This greater threat looming from the East has led Western financial entities and critical infrastructures alike to step up their level of preparedness for potential cyber attacks. In verifying whether a sufficient level of cyber resilience has been achieved and strengthening the defensive measures where needed, the TIBER-BE programme has proven to be a valuable tool. Through the threat-intelligence-based scenarios making up a TIBER-BE engagement, real and relevant threat actors and the techniques they use are emulated. This enables the tested entities to identify and remediate weaknesses that are most likely to be targeted and exploited by these selected threat actors.

After three years of TIBER testing, all entities in the initial scope of the programme have been subjected to a TIBER-BE engagement. While setting up a new initiative like this may be challenging, all tests performed so far can be deemed successful, with a number of lessons learnt for all entities involved. The success of this first cycle helped to establish the framework's reputation and clears the way for subsequent rounds of TIBER-BE testing. The increased credibility brought by the successful first round of TIBER-BE engagements has enabled the programme to grow both in size and thoroughness of the testing approach. For the second round of testing, several new entities have been added to the scope of the programme. This extension has consequently improved the coverage of TIBER testing, further bolstering the programme's ability to enhance the Belgian and European financial system's cyber resilience. Additionally, for those entities that have already completed a TIBER-BE engagement, the experience from the first test has enhanced their familiarity with the TIBER framework which should lead to greater willingness on their part to go through more extensive and more thorough TIBER tests in the future.

BOX 13

Improving implementation of TIBER-BE

Key to improving the TIBER-BE initiative and the willingness of financial entities to be involved in it is the ability to provide feedback and insight as to how to maximise the return on investment of a TIBER-BE test. Feedback helps the NBB to pinpoint areas where the implementation of TIBER-BE can be improved and make adaptations where possible. For this reason, the TIBER-BE programme has singled out a number of ways through which feedback can be shared. This includes (i) a dedicated feedback workshop at the end of TIBER-BE engagements, (ii) a National Implementation Committee where all financial entities falling under the scope of the TIBER-BE programme are invited to share their views on the TIBER framework with the NBB and each other, and (iii) participation of the TIBER-BE team in the TIBER Knowledge Centre, an international committee where all countries that have implemented the TIBER-EU framework come together to exchange insights, best practices and lessons learnt. Feedback obtained through the above-mentioned channels led to the review and rewrite of the TIBER-BE National Implementation Guide, the official TIBER-BE document that was published on the NBB's website in December 2022.

EDITORIAL COMMITTEE

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) https://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. https://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. https://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. https://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
	Regulation (EU) 2022/858 of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology, and amending Regulations (EU) No. 600/2014 and (EU) No. 909/2014 and Directive 2014/65/EU. (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0858)

FMIs	**Regulation (EU) 2022/2554 of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No. 1060/2009, (EU) No. 648/2012, (EU) No. 600/2014, (EU) No. 909/2014 and (EU) 2016/1011 (14 December 2022):** DORA seeks to harmonise approaches across the financial sector with the objective of an increased digital operational resilience and to ensure a safer and more stable overall financial system. A broad range of financial entity types falls under the scope of DORA, including central securities depositories, credit institutions, insurance and reinsurance undertakings, investment firms, payment institutions and electronic money institutions. (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2554)
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. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012R0648&from=EN
	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. https://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. https://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

CCPs	**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. https://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 https://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 https://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/revisedoversightframeworkretailpayment systems201602.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. https://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. https://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. https://www.ejustice.just.fgov.be/eli/arrete/2019/01/25/2019030120/moniteur **(FR)** or https://www.ejustice.just.fgov.be/eli/besluit/2019/01/25/2019030120/staatsblad **(NL)**

Card Payment Schemes	Payment Instruments, Schemes, and Arrangements (PISA Oversight framework, November 2021) https://www.ecb.europa.eu/paym/pdf/consultations/ecb.PISApublicconsultation202111_1.en.pdf
	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. https://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/eli/wet/2016/12/01/2016011497/staatsblad (NL) ■ https://www.ejustice.just.fgov.be/eli/loi/2016/12/01/2016011497/moniteur (FR)
	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

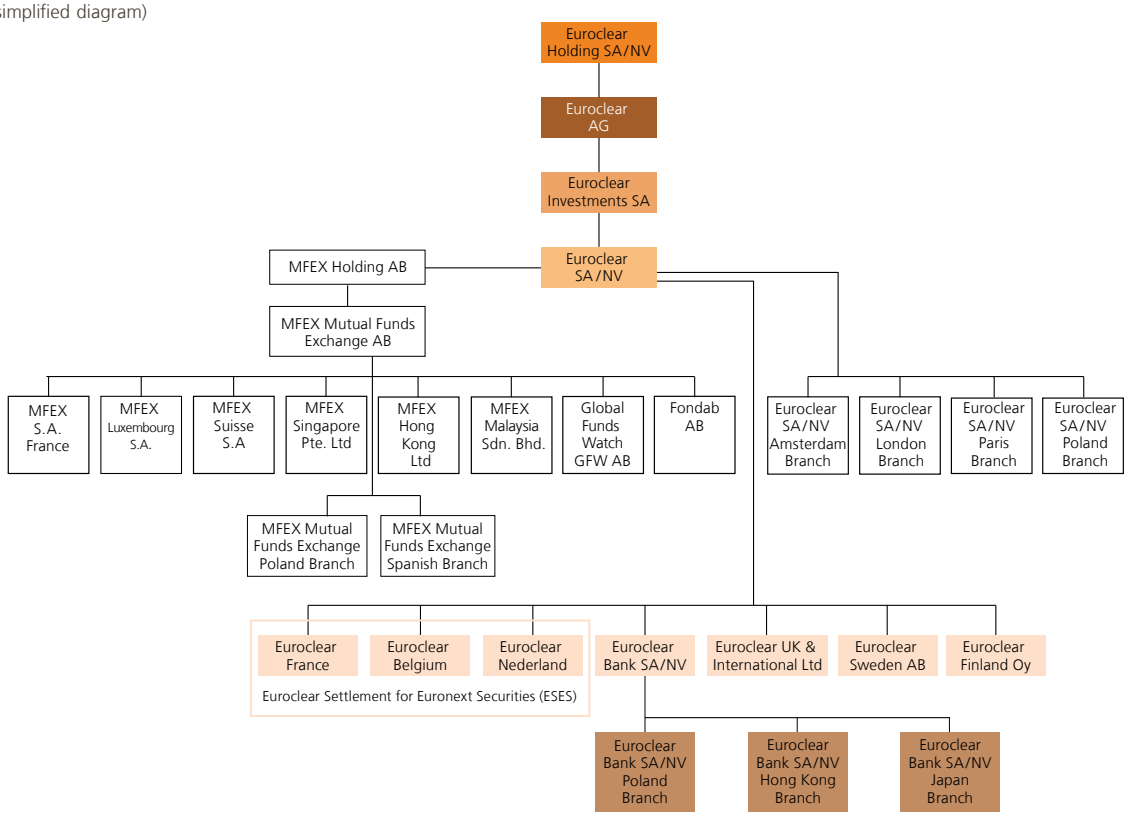
Euroclear Holding SA/NV, the top financial holding of Euroclear, is incorporated under Belgian law. Euroclear Holding SA/NV owns 100 % of Euroclear AG, a Swiss financial holding company. Euroclear Investments SA is the group's financial investment holding company, incorporated in Luxembourg.

Euroclear SA/NV (ESA), a Belgian financial holding company, is the parent company of the Euroclear Group (I)CSDs: i.e. the three ESES CSDs (Euroclear France, Euroclear Nederland, Euroclear Belgium), Euroclear UK & International Ltd, Euroclear Sweden AB, Euroclear Finland Oy and Euroclear Bank SA/NV. The latter has branches in Poland, Hong Kong and Japan. The Euroclear group completed the acquisition of MFEX Group, a global digital fund distribution platform, on 15 September 2021.

Chart 1

Euroclear Group Corporate Structure

(simplified diagram)



Source: Euroclear.

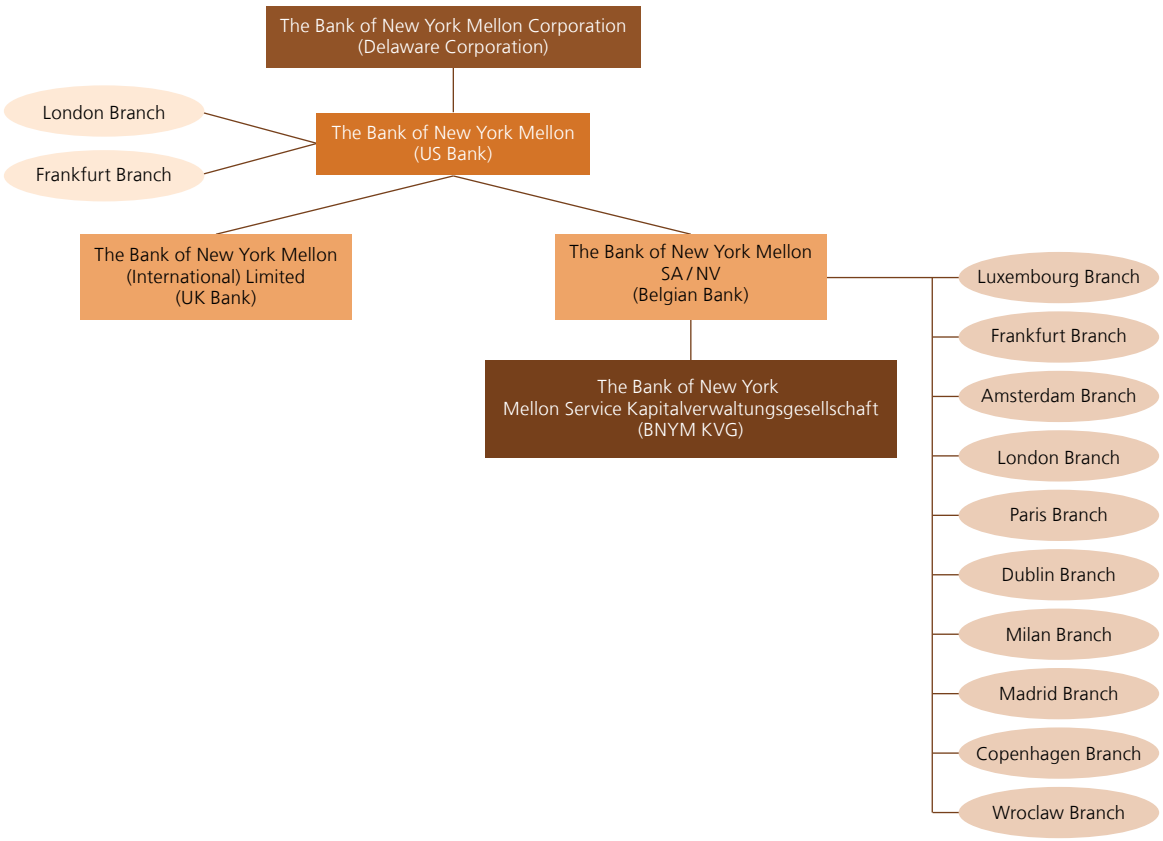
The Bank of New York Mellon

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 – situation end 2022)



Source: BNY Mellon.

Worldline

Worldline is a French group providing electronic payment and transactional services in Europe and beyond.

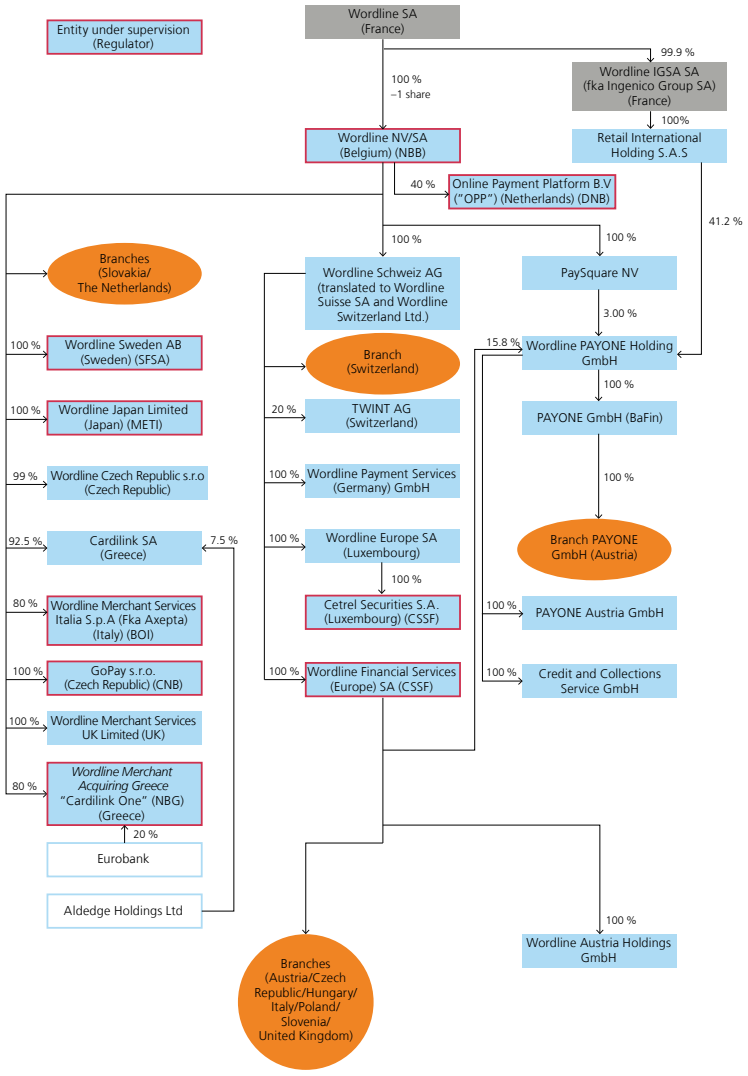
In 2016, Worldline SA/NV, the Belgian entity of the group merged with the Dutch company Equens. The processing activities were carved out in a new entity called equensWorldline SE. equensWorldline SE is now a full subsidiary of Worldline SA (France).

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). 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 20 March 2023, simplified diagram, part of the group relevant for Belgium)



Source: Worldline.

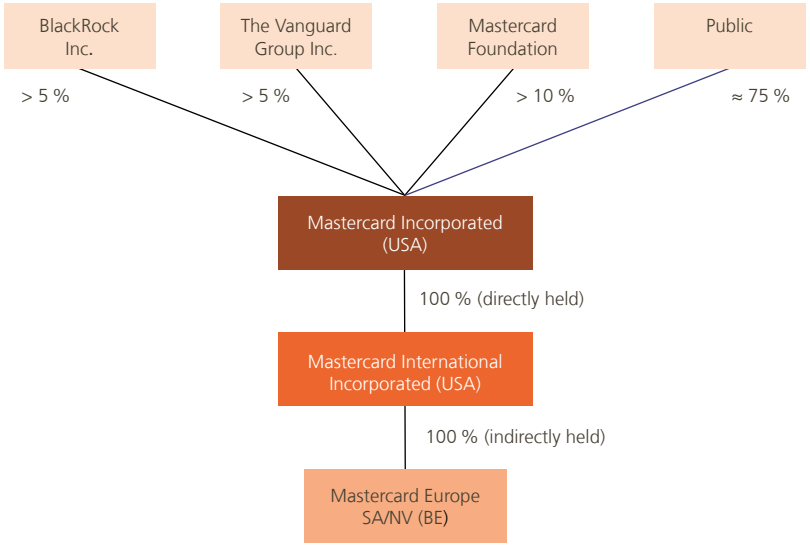
Mastercard Europe

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

Chart 4

Mastercard Group Structure

(simplified diagram, as of January 2023)



Source: Mastercard Europe.

Annex 3: Statistics

List of tables

Table 1

Securities Settlement and Custody

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

	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
A. Euroclear Bank										
Value of securities deposits (end of period)	10 834.2	11 765.3	12 393.7	12 698.4	12 834.2	13 451.5	14.823.6	15.292.4	17.105.3	17 528.3
Number of transactions (in millions)	69.5	75.2	83.3	84.1	95.4	107.0	116.4	128.8	146.9	163.3
Value of transactions	336 784.6	394 569.3	442 563.0	451 698.3	498 181.0	525 692.4	544.564.8	575.991.9	652.617.0	692 212.8
Source: Euroclear.										
B. NBB-SSS										
Value of securities deposits (end of period)	541.7	557.3	575.4	612.5	625.3	632.6	646.65	698.66	727.1	772.1
Number of transactions (in millions)	0.6	0.6	0.5	0.5	0.5	0.5	0.5	0.5	0.6	0.6
Value of transactions [1]	8 428.0	8 209.0	8 766.5	8 714.5	9 069.8	11 043.7	8 512.6	9 220.7	11 543.3	11 599.2
Source: NBB. 1 Secondary market turnover.										
C. Euroclear Belgium										
Value of securities deposits (end of period)	202.7	222.1	269.4	235.1	237.7	178.0	220.2	194.9	218.9	193.3
Number of transactions (in millions)	1.9	2.1	2.5	2.4	2.5	2.7	2.6	2.9	2.7	2.6
Value of transactions	799.8	714.8	944.6	963.8	946.0	964.1	783.9	704.9	722.4	735.1
Source: Euroclear.										
D. TARGET2-Securities [1]										
Number of transactions (in millions)	nap	nap	7.6	36.3	125.6	145.9	154.8	176.7	187.4	181.9
Value of transactions	nap	nap	43 706.8	112 066.0	192 175.0	236 050.8	282 063.7	172 840.9	178 304.1	184 184.5
Source: ECB. T2S was launched in 2015. 1 As of 2020, the data in this table excludes technical transactions in T2S and liquidity transfers from traffic statistics.										
E. BNYM SA/NV										
Value of assets held under custody (end of period)	2 905.2	3 454.0	3 216.4	3 476.5	3 608.8	2 373.1	2 873.5	2 903.5	3 290.4	2 834.4
Source: BNYM.										

Table 2

Payments

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

	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
A. TARGET2										
Value of payments	559 696.0	498 726.5	508 982.3	485 811.8	432 780.7	432 508.1	441 281.1	465 793.7	484 251.6	570 539.0
of which: TARGET2-BE	16 177.3	16 247.9	15 627.4	16 957.9	19 732.4	22 594.7	24 935.5	28 570.6	27 921.2	29 411.7
Number of payments (in millions)	91.3	87.8	88.6	89.0	89.3	88.4	87.8	88.7	96.4	102.6
of which: TARGET2-BE	2.3	2.5	2.3	2.2	2.3	2.3	2.5	3.1	3.3	3.3

Source: ECB Payment Statistics. RTGS related payments, excluding TARGET2 transactions on Dedicated Cash Accounts.
Last year's figures from https://www.ecb.europa.eu/stats/payment_statistics/large_value_payment_systems/html/index.en.html.

B. CLS										
Value of payments (in € trillion)	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	1 361 618.0	1 597 910.9
of which: EUR payments	182 305.8	191 170.5	208 555.8	204 370.7	219 924.6	241 067.1	249 090.1	244 744.0	254 388.0	292 542.1
Number of payments (in millions)	205.0	204.7	219.1	209.5	198.5	226.6	257.1	273.5	252.7	301.0
of which: EUR payments	36.9	34.4	40.9	34.3	34.0	39.1	42.2	45.4	41.2	50.8

Source: CLS.

C. Centre for Exchange and Clearing (CEC)										
Value of payments (exclusive Instant Payments since 2020[1]) (in € billion)	911.6	870.7	883.4	920.6	941.8	1 122.9	1 204.7	1 198.8	1 309.2	1 394.0
Value of Instant Payments (in € billion)	nap	nap	nap	nap	nap	nap	nap	57.2	75.1	82.8
Number of payments (exclusive Instant Payments since 2020[1]) (in millions)	1 365.6	1 272.2	1 402.2	1 387.1	1 312.0	1 456.7	1 512.7	1 396.9	1 467.8	1 395.0
Number of Instant Payments (in millions)								99.6	125.2	148.0

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)

	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
D. Payment Institutions (PIs) – Electronic Money Institutions (ELMIs)										
PIs										
Belgian PIs	11	15	17	21	24	22	26	30	30	29
Account information services providers							1	3	4	6
Foreign PIs with Belgian branch	2	3	3	3	2	3	4	5	6	7
Passport notifications for cross-border services of foreign EEA PIs towards Belgium	184	262	273	379	421	435	511	566	276 [1]	307
ELMIs										
Belgian ELMIs	10	10	10	8	8	7	7	7	6	5
Foreign ELMIs with Belgian branch	0	1	1	1	1	2	1	1	1	1
Passport notifications for cross-border services of foreign EEA ELMIs towards Belgium	40	54	53	102	156	188	240	278	162 [1]	183
Institutions offering services within a limited network (new under PSD2)						1	4	5	5	9
Transactions by Belgian PIs and ELMIs (in millions)										
Number of transactions (yearly total)	1 665	1 874	1 968	2 155	2 006	2 044	1 949	2 106	2 358	2 595
Value of transactions in euro (yearly total)	105 989	133 513	136 567	137 144	124 388	124 485	113 639	121 751	177 792	202 155
Average outstanding E-Money of Belgian ELMIs	15.2	21.8	35.8	45.5	73.9	116.6	405.2	494.3	481.7	302.8
Number of transactions of Money Remittances (yearly total, in millions)							5.7	11.2	31.0	nav
Value of Money Remittances (in millions)							1 546	3 043	17 304	nav
E. Processors of payment transactions										
Worldline SA/NV										
Number of transactions (yearly total, in millions) [1]	1 553.9	1 665.8	1 800.0	1 960.0	2 150.0 1 746	1 774	1 940	1 972	2 310	2 708

Source : NBB.

1 Decrease as consequence of the Brexit.

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

	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
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	35 179.2	41 243.9	42 640.8	nav
Number of cards per capita (end of period)		1.9	1.9	2.0	2.0	2.1	3.1	3.6	3.7	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	44.4	38.6	40.2	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	1 853.5	1 559.8	1 572.3	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	202.3	213.2	238.7	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	9.3	10.3	nav

Source : ECB Payment Statistics.

1 Except cards with an e-money function.

G. Card schemes										
Bancontact – Number of transactions (yearly total, in millions)	1 180.4	1 241.8	1 306.7	1 389.5	1 441.6	1 480.2	1 593.4	1 706.1	1 982.2	2 270.3
of which :										
Payments	1 068.4	1 125.9	1 190.9	1 272.8	1 325.2	1 336.0	1 488.8	1 637.5	1 910.2	2 187.9
ATM [1]	111.9	115.9	115.9	116.8	116.3	114.2	104.6	68.6	72.2	82.4

Source : Bancontact.

1 Until 2021 figures regarding ATM withdrawals reported by Bancontact did not include "on-us" operations (i.e. withdrawals made at an ATM operated by the issuer of the card used). Since 2022, on-us withdrawals of KBC, ING, BNP Paribas Fortis and Belfius made on ATMs operated by Batopin (their common ATM network provider) are included in the figures.

Table 3

Swift

(yearly total, in millions)

	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
Number of messages	5 065.7	5 612.7	6 106.6	6 525.8	7 076.5	7 873.6	8 454.4	9 526.5	10 593.7	11 254.9
of which:										
Payment messages	2 524.5	2 737.2	2 930.2	3 139.3	3 485.2	3 840.0	4 053.4	4 313.0	4 799.5	4 992.8
Securities messages	2 215.6	2 545.2	2 829.1	3 019.1	3 232.3	3 635.5	3 968.9	4 709.8	5 269.2	5 714.8
Other messages	325.6	330.3	347.3	367.3	359.0	398.1	432.1	503.8	525.0	547.3

Source: Swift.

List of abbreviations

AIFMD	Alternative Investment Fund Managers Directive
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
ATM	Automated teller machine
BCBS	Basel Committee on Banking Supervision
BIC	Bank Identifier Code
BNYM	Bank of New York Mellon
CASP	Crypto-asset service provider
CBDC	Central bank digital currency
CCP	Central counterparty
CCP-RR	CCP recovery and resolution
CEC	Centre for Exchange and Clearing
CER	Critical Entities Resilience Directive
CLS	Continuous Linked Settlement
CO_2	Carbon oxide
CPMI	Committee on Payments and Market Infrastructures
CPS	Card Payment Scheme
CRD	Capital Requirements Directive
CROE	Cyber Resilience Oversight Expectations for FMIs
CRR	Capital Requirements Regulation
CSC	Common and Secure Communication
CSCF	Customer Security Controls Framework
CSD	Central Securities Depository
CSDR	CSD Regulation
CSP	Customer Security Programme
CSRD	Corporate Sustainability Reporting Directive
DDoS	Distributed denial-of-service
DG FISMA	Directorate-General for Financial Stability, Financial Services and Capital Markets Union
DLT	Distributed Ledger Technology
DORA	Digital Operational Resilience Act
DR	Depository receipts
DVP	Delivery versus payment
EBA	European Banking Authority
EC	European Commission

ECB	European Central Bank
EEA	European Economic Area
EIS	EU Issuance Service
ELMI	Electronic money institution
EMEA	Europe, Middle East and Africa
EMIR	European Market Infrastructure Regulation
EMT	Electronic money token
EPI	European Payments Initiative
ERPB	Euro Retail Payments Board
ESA	Euroclear SA/NV
ESAs	European Supervisory Authorities (EBA, ESMA and EIOPA)
ESCB	European System of Central Banks
ESES	Euroclear Settlement of Euronext-zone Securities
ESMA	European Securities and Markets Authority
ESG	Environmental Social Governance
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
HLE	High Level Expectation
HLTF – CBDC	High-Level Task Force CBDC
ICSD	International central securities depository
ICT	Information and Communication Technology
IOSCO	International Organisation of Securities Commissions
ISAC	Information sharing and analysis centre
IT	Information Technology
JST	Joint Supervisory Team
LVPS	Large-Value Payment Systems
MAG	Market Advisory Group
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
NFC	Near Field Communication
NGEU	NextGenerationEU
NIS	Network and Information Security
NRPC	National Retail Payments Committee
OC	Oversight Committee

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
PSG	Project Steering Group
PSP	Payment Service Provider
PSU	Payment Service User
PVP	Payment versus payment
RPS	Retail payment system
RTS	Regulatory Technical Standard
SCA	Strong Customer Authentication
SCT	SEPA credit transfer
SDR	Settlement Discipline Regime
SEPA	Single European Payments Area
SI	Systemically-relevant credit institution
SIPS	Systemically important payment system
SREP	Supervisory Review and Evaluation Process
SSM	Single supervisory mechanism
SSS	Securities settlement system
Swift	Society for Worldwide Interbank Financial Telecommunication
T2S	TARGET2-Securities
TIBER	Threat Intelligence Based Ethical Red Teaming
TFCD	Task Force on Climate-related Financial Disclosures
TPRM	Third-party risk management
TPP	Third-party provider
UCITS	Undertakings for Collective Investments in Transferable Securities Directive

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 2023

Printed on FSC paper