

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 instruments¹, payment schemes² 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: T2³ 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~f5c7bdf6d.en.html>.

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

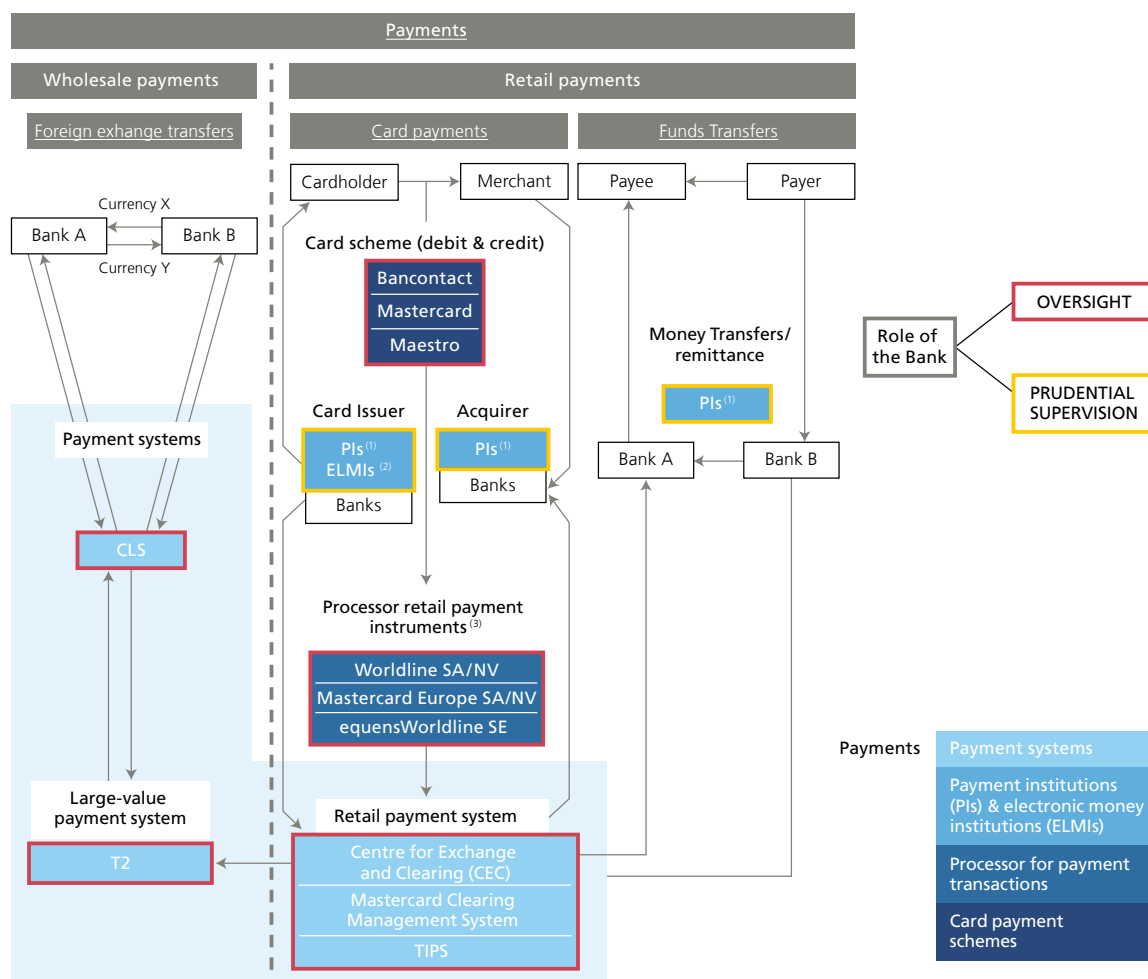
As an acquirer¹ and processor of retail payment instruments in Belgium, Worldline SA/NV is subject to both prudential supervision and oversight. The Bank's activities in that respect are covered in section 3.3.

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 (CROE¹) 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 Systems² 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 money¹. 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 money².

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 2022³.

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 & CSC⁴. 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 Circular⁵ 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.

Need for a revision of the second payment services directive?

The revised Payment Services Directive¹, 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 laws². 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 review³.

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 2022 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 online¹, 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 AISP's business models. Today's PSD2 rules foresee in a voluntary 180-day exemption² (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 requirement³. The amount is calculated in line with EBA Guidelines⁴ 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 law¹ 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 institutions². 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 published 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 institutions¹ were granted a licence, one institution changed its licence² and four institutions were withdrawn³ 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 Odo Finance NV, Freedely 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 Strategy¹, 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 field³.

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 stated¹, 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 services² 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 legislation¹, the European Supervisory Authorities² 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 ARTs³ 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 process⁴) 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 assumptions⁵, 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.

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 2021¹. Moreover, a regular dialogue on a digital euro has been established with all market participants², 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 public¹ 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 – EPI³: 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 Eurosystem¹. The PISA oversight framework was designed with the objective of addressing technological developments in the payment industry. The framework² itself is complemented by an assessment methodology³ and an exemption policy⁴. 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.