E. Digitalisation

The year 2020 brought an acceleration in digital access to financial services, electronic and contactless payments, e-commerce and the use of digital infrastructures, enabling consumers, workers and firms to cope with the unprecedented situation created by the COVID-19 pandemic. The security and continuity of the financial sector's digital infrastructures thus became even more crucial, and the importance of digital innovation as a factor in economic recovery became clear with the more rapid development of remote forms of consumption. There were various apparent trends in innovation in digital finance. Examples include new business models based on innovative payment solutions, the operational efficiency drive via the use of artificial intelligence, Machine/Deep Learning and Robotic Process Automation, refinement of commercial strategies using data analysis and artificial intelligence, and the positioning of IT infrastructures and data aggregation in the cloud. These developments are often intended to anticipate fundamental changes expected in the structure of the financial services market. The role of financial services and players in the global market for products and services is in fact changing rapidly throughout the world. There is a progressive shift towards a market in which financial and non-financial services are based on integrated payment, e-commerce and social media platforms, and cooperative ecosystems comprising these various dimensions. Factors facilitating these changes include the use of modular technologies enabling various financial and non-financial players to communicate via interfaces (application programming interfaces – APIs). The initiatives relating to global stablecoins which will facilitate payments through such ecosystems and platforms are taking shape. For instance, in April 2020, the Libra Association (renamed Diem) published a new version of its White Paper in an effort to respond to the concerns expressed by various supervisory bodies, central banks and other stakeholders. In April 2020, it submitted an application to the Swiss financial regulator (*Autorité fédérale de surveillance des marchés financiers* – FINMA) for authorisation as a payment system.

These trends are already exacerbating certain risks (such as cyber risk and IT risks) and creating new ones for consumers, monetary policy and financial stability, or they could do so in the short or medium term. In that context, the European Commission published a digital strategy with a view to encouraging digital innovation, the creation of a single digital market in financial services, and a European area for financial data stimulating access to and the sharing of such data, and greater control over the risks resulting from digital innovation. In September 2020 this led to the first legislative initiatives, with which the Bank is closely involved. Two of them – concerning operational resilience and crypto-assets – are discussed below. Various consequences of these developments and the importance of digital finance – such as the increase in cyber and IT risks, open banking and the rules on strong customer authentication included in the second Payment Services Directive (PSD2) – are also examined, as well as the initiatives relating to the digital euro.

1. Digital operational resilience

1.1 Continuing rise in cyber risks and IT risks

During the year under review, the digital operational resilience of the financial sector was tested to a considerable degree by the COVID-19 pandemic. From March 2020 onwards, institutions asked (or required) their staff to work from home whenever possible: that poses unprecedented challenges and presents additional risks. At first, the challenges were mainly operational, such as the need to extend IT capacity to permit remote working on a large scale. As the pandemic dragged on, the challenges took a more strategic turn. For instance, institutions were forced to set priorities between current and planned strategic projects, because the current circumstances often do not permit maintenance of the pace and extent of change prevailing before the health crisis. While widespread remote working reduces the health risk, it heightens the inherent cyber risks and IT risks, e.g. because the smaller number of operators physically present makes it more difficult to resolve incidents, but also because of the large number of company computers simultaneously connecting remotely to the institution via the internet. Fortunately, thanks to the precautions that the institutions took, there were no serious operational incidents during the year under review.

The security and continuity of the financial sector's digital infrastructures became even more crucial in 2020

Throughout the world, cyber attacks have become an everyday reality in recent years. At the same time, attackers are evidently refining the techniques and methods used, so that some of the attacks are becoming ever more sophisticated and powerful. The number of persistent, targeted cyber attacks is therefore likely to increase further in the future,

with the financial sector logically remaining one of the potential targets. The list of cyber attacks targeting financial institutions worldwide, drawn up by the think tank, the Carnegie Endowment for International Peace[1], indicates the current situation concerning the cyber threats facing the sector. In 2020, for example, the attacks mentioned aimed to steal sensitive data such as loan applications and credit card numbers, to disrupt ATM systems and to initiate fraudulent transactions by breaking into banks' server systems.

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

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

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

1.2 Legislative guidelines and developments

In recent years, the Bank has made a substantial contribution to a regulatory framework aimed at improving the control of cyber risks and IT risks. The prudential circular on the Bank's expectations concerning operational business continuity and security of systemically important institutions[2] remains a key reference point. The Bank also makes an active contribution to establishing a European regulatory framework for the management of cyber risks and IT risks. Under the aegis of the EBA, this resulted in the publication of the EBA guidelines for supervisory authorities on the assessment of the ICT

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

2 Circular NBB_2015_32 of 18 December 2015 on additional prudential expectations concerning the operational continuity and security of systemic financial institutions.

risk in the SREP[1], guidelines on outsourcing[2], and guidelines on ICT and security risk management[3]. These guidelines have now all become part of the Bank's supervision and policy framework. For insurers, the Bank also contributes to the establishment of a similar regulatory framework under the auspices of EIOPA. In 2020, the guidelines on outsourcing to cloud service providers[4] were transposed in an NBB Circular, and guidelines on ICT security and governance[5] were published.

In September 2020, the European Commission published a proposal for a Regulation called the Digital Operational Resilience Act (DORA). This proposal aims to mitigate the risks associated with the digital transformation of the financial sector by laying down strict, common rules on governance and ICT risk management, ICT incident reporting and information sharing, security tests and ICT risks relating to third parties. These rules would apply to a wide range of financial institutions, but also to critical ICT service providers (third-party providers), such as cloud service providers, who would be subject to a form of oversight. As a member of the Belgian delegation, the Bank plays an important advisory role in discussions on draft texts at European level and will probably also be closely involved in the subsequent transposition of the European DORA Regulation into technical standards.

1.3 Operational activities

Assessing cyber risks and IT risks and encouraging control over those risks are top priorities for the Bank, and European and international cooperation in that sphere is becoming increasingly important. Here, the Bank focuses on the security of individual financial institutions and FMIs and the confidence that they inspire, and on cross-sectoral control strategies.

The approach concerning individual institutions is two-pronged. On the one hand, institutions subject to prudential supervision are required to hold capital to cover their operational risks, including cyber risks and IT risks. Also, 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. In 2020, the Bank conducted a number of inspections (for banks under the SSM) to check on compliance with the regulatory framework and the proper management of IT systems in relation to cyber risks and IT risks. In addition, the Bank monitors these risks in financial institutions and FMIs in the course of its ongoing and recurrent supervisory activities. The COVID-19 health crisis obliged the Bank to revise its approach to these supervision activities. On the one hand, the content of the activities was adjusted to the new reality, with particular emphasis on COVID-19, while working methods were also adapted to give preference where possible to remote meetings and technological resources.

In 2018, the Bank established a framework for ethical hacking, known as TIBER-BE (Threat Intelligence-Based Ethical Red Teaming Belgium). This programme forms the Belgian part of a methodology devised by the Eurosystem and aims to boost individual financial institutions' and FMIs' cyber resilience by means of sophisticated tests, and to supply important insight into the cyber security of the Belgian financial sector as a whole. The Bank encourages these exercises in its capacity as the guardian of financial stability. During the year under review, an updated version of the TIBER-BE framework was published on the Bank's website, in which the methodology is refined on the basis of the experience gained from tests already carried out. The sector seems convinced of the soundness of the methodology used and the benefits offered by these specific tests. Meanwhile, the TIBER-BE team has also successfully conducted cross-border tests, in close and effective collaboration with other EU countries which have implemented the TIBER framework, and with the UK, in seeking synergies with the similar CBEST framework. TIBER-BE is now fully operational.

The Bank is also paying closer attention to sectoral initiatives. For example, under the SSM, it regularly conducts transversal analyses on cyber- and IT-related subjects. In 2020, all significant banks and some less significant banks were again asked to complete an IT questionnaire which provides important data for the annual Supervisory Review and Evaluation

1 EBA Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation Process (SREP) (May 2017).
2 EBA Guidelines on outsourcing arrangements (February 2019).
3 EBA Guidelines on ICT and security risk management (November 2019).
4 EIOPA Guidelines on outsourcing to cloud service providers (February 2020).
5 EIOPA Guidelines on information and communication technology security and governance (October 2020).

Process (SREP) and also permits cross-sectoral analyses. A large number of insurance undertakings and investment firms were also asked to provide such information for a similar purpose.

In its role as the sectoral authority for application of the law on the security and protection of critical infrastructures (principally systemic banks and FMIs), the Bank also assesses the effectiveness of the control systems of these critical financial infrastructures. In that context, the Bank likewise organises and coordinates sectoral crisis simulation exercises in order to prepare the Belgian financial sector for potential operational incidents of a systemic nature. Under the law on network and information system security (NIS), the Bank acts as the sectoral point of contact for incidents in the financial sector.

2. FinTech

2.1 Strong customer authentication and open banking

The main supervisory activity in regard to payments consists in monitoring compliance with the stricter security requirements for electronic card payments in e-commerce and facilitating access to the payment account systems of credit institutions for FinTech players.

2.1.1 Strong customer authentication: continuing activities

The introduction of the rules on strong customer authentication (SCA) in September 2019 caused a number of implementation problems for the online card payments sector (e-commerce).

On the one hand, in some cases payment card issuers (primarily credit institutions) need to modify their payment card authentication procedures to conform to these rules; also, online card transactions must now normally be authenticated, which was not always the case. This latter obligation requires the introduction of new technical protocols in a complex ecosystem with numerous players. These protocols permit authentication and correct use of the legal exceptions to strong customer authentication and ensure that all players in the sector can correctly authenticate each card transaction.

The adjustments that online merchants must make in order ensure that their websites duly support these protocols on their websites in all cases and on time in order to permit the authentication of card transactions present a particular challenge for the sector. Since Belgian payment card holders transact business online with foreign merchants in neighbouring countries, the migration to SCA for those merchants is an equally crucial factor for the success of that migration in Belgium.

In order to steer this migration in the right direction and in accordance with the EBA's opinion on the subject, the Bank had already granted the Belgian card payments sector postponement of the implementation of the SCA rules in August 2019, and drew up a national migration plan in consultation with the sector, under the direction of Febelfin. That plan was published on the Bank's website in May 2020. The national migration plan resolutely opted for a gradual transition to full application of SCA to all card transactions. During a transitional period, a "soft refusal" system will apply to card transactions, meaning that transactions which exceed a certain amount (e.g. € 1 500) presented to the card issuer by an online merchant (and its acquirer) without authentication of the card holder will be refused, with a request to resend it to the card issuer but this time with authentication of the card holder. The card holder is unaware of this "soft refusal" unless the merchant has not yet incorporated the necessary protocols in his web shop, in which case the transaction cannot proceed ("hard refusal"). The thresholds for applying this procedure will be gradually lowered during the transitional period until full conformity with the SCA rules is achieved at the end of that period.

The Bank is actively monitoring the implementation of this migration plan, in cooperation with the sector, and is making any necessary adjustments. In this connection it takes account of parameters such as the experience of Belgian card issuers in gradually tightening up the authentication rules in accordance with the migration plan, and the speed with which online merchants in Belgium and elsewhere migrate to the required technical protocols.

The stricter security requirements for electronic payments and FinTech access to payment account systems have been closely monitored

2.1.2 Open Banking: access to payment account systems

A second important supervision activity in 2020 concerned checks on compliance with the rules on the access of FinTech players to payment accounts held with credit institutions.

The second Payment Services Directive (PSD2) introduced two new categories of regulated service providers, namely payment initiation service providers and account information service providers (collectively known as "third parties"), who – after respectively obtaining the authorisation or recognition of the Bank (or another competent authority in the EEA) – are, subject to the consent of the account holder(s), respectively entitled to initiate payments from payment accounts held with credit institutions and to aggregate information on those accounts.

To ensure that this is technically feasible for these third parties, credit institutions must create a technical access channel (dedicated interface) which these third parties can use in order to offer their services. The technical requirements were defined in the technical standard relating to SCA & CSC[1], which came into force on 14 September 2019.

In 2020, the EBA found that there was still uncertainty on the market regarding the interpretation of the ban on creating or providing for obstacles for these third parties in the technical operation of these dedicated interfaces. In June 2020 this resulted in an EBA opinion on obstacles and their elimination.

The Bank endorsed this EBA opinion and in a Communication dated 1 July 2020 it made clear that it takes that opinion as the basis of its interpretation of the ban on obstacles for third parties and that it expects credit institutions to eliminate all barriers in their dedicated interfaces by 31 December 2020. The Bank is actively monitoring the elimination of these

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

barriers by credit institutions and providing technical clarification where necessary.

2.2 The digital euro

The European central banks are examining various prospective scenarios in which issuance of a digital euro – a central bank digital currency (CBDC) – is advisable or necessary. These scenarios include, for example, a steep decline in the use of cash (notes and coins) as a means of payment, a significant rise in the use of unregulated means of payment resulting in a serious threat to financial stability and consumer protection, or a substantial increase in the use of digital money issued by foreign central banks sufficient to compromise the euro's position.

In October, the ECB in collaboration with experts from 19 national central banks in the euro area published a report listing and assessing the prospective scenarios identified. That report also contains some basic principles for possible issuance. A digital euro can only supplement the existing means of payment (e.g. cash) and must not discourage or impede private initiatives. No decision has yet been taken on the issuance of a digital euro.

2.3 Draft EU Regulation on markets in crypto-assets (MiCA)

In September 2020 the European Commission published a proposal for a Regulation on Markets in Crypto Assets (MiCA). This proposal forms part of its digital strategy.

The European Commission published a proposal for a Regulation aimed at creating a framework for crypto-assets

With this Regulation, the Commission aims to create a framework for crypto-assets which cannot be classed as financial instruments, electronic money, deposits, structured deposits or securitisation instruments, and for crypto-asset services not already covered by the rules in force.

The first section of the proposal contains rules on the offering and admission to trading of certain crypto-assets on a trading platform within the EU, plus rules on the issuers. These rules vary according to the crypto-asset category. The MiCA divides crypto-assets into three categories: 1° crypto-assets backed by a currency which is legal tender, the issuer being a credit institution or electronic money institution ("e-money tokens"), 2° assets backed by a basket of currencies which are legal tender, one or more commodities, one or more crypto-assets, or a combination of those assets, and comprising a stabilisation mechanism ("asset-referenced tokens"), 3° other crypto-assets which do not belong to either of the first two categories of crypto-assets. The first two asset categories are intended mainly for stablecoin issuers, while the third fulfils the aim of the Regulation to create a framework for all crypto-assets (other than those already regulated) issued by any one issuer, whatever their nature. In the case of the first two asset categories, the issuer must obtain prior authorisation. That regime is organised by the MiCA for asset-referenced tokens and governed by the Directives applicable to the institutions concerned in the case of e-money tokens. In the case of asset-referenced tokens, the White Paper[1] must first be approved, while prior notification of the White Paper is required in the case of e-money tokens. In contrast, assets in the "other" category are subject to rules on prior notification of the White Paper and to certain requirements concerning the issuer. Only in the case of these assets will the competent authority conduct retrospective checks on compliance with the requirements. Finally, the issuers are subject to rules of conduct and transparency and prudential requirements.

For the first two asset categories, special rules apply if the asset is regarded as significant on account of criteria indicating a bigger impact, particularly for financial stability. In that case, the European Banking Authority would be the competent authority for those assets in regard to some or all of the provisions of the Regulation.

Finally, a second section contains rules on crypto-asset services such as custody and administration, operation of a trading platform, execution of orders, etc.

The Bank is closely involved in the negotiations on this proposal in its capacity as an expert at the Permanent Representation of Belgium to the European Union.

1 The White Paper is a document that is drafted and published by the issuer under its responsibility and that contains the most important information that must be published in accordance with the MiCA (e.g. with regard to the issuer, the project, the type of asset and the rights on that asset, or the technology) in order to allow the future buyer of the crypto-asset to make an informed purchase decision.