# D. Digitalisation

The digitalisation of financial services continued to gain importance in 2021, as it enables consumers, workers and businesses to cope with the challenges associated with the COVID-19 pandemic. Many trends are becoming apparent in terms of innovation. For example, there are new business models based on innovative payment solutions, the quest for operating efficiency via the use of machine/deep learning or robotic process automation, refinement of commercial strategies via data analysis and artificial intelligence, and the positioning of IT infrastructures and data aggregation in the cloud. These trends often reflect the aim of anticipating the fundamental changes expected in the structure of the financial services market, as the role of financial services and players is changing significantly at global level. There is a progressive shift towards a market in which financial and non-financial services are structured around integrated payment, e-commerce and social media platforms, with cooperative ecosystems covering these various aspects. These developments are facilitated in particular by the use of modular technologies enabling different financial and non-financial players to communicate via interfaces (application programming interfaces – APIs). Theinitiatives concerning global stablecoins which will facilitate payments in such ecosystems and platforms are taking shape.

*Digitalisation is already having a major influence on the risks facing financial institutions and financial stability*

These developments are already having a major influence on the risks facing financial institutions, and on consumers, monetary policy and/or financial stability. Since digitalisation leads to greater interconnectivity, (cyber) security and the continuity of the underlying systems and infrastructures are more crucial than ever. There is every indication that the risks inherent in digitalisation will only increase in the foreseeable future.

In that context, the European Commission proposed a digital strategy designed to boost digital innovation, creation of a single digital market in financial services and a European financial data area encouraging access to and sharing of those data. That strategy also aims to achieve better control of the risks resulting from digital innovation. In September 2020, it led to a series of European legislative initiatives in which the Bank was closely involved.

Two of them, relating to operational resilience and crypto-assets, are examined below. Other sections look at the implementation of open banking, governed by the second Payment Services Directive (PSD 2), and at the regulatory initiative aimed at defining harmonised rules on artificial intelligence, launched by the European Commission in April 2021. This chapter likewise deals with the action taken by the Bank to support the ECB's initiative concerning the digital euro, and the efforts made to map FinTech/InsurTech developments in supervised institutions and to limit the cyber risks and IT risks to which they are exposed.

## 1. FinTech

### 1.1 Open banking: access to payment account systems under PSD 2

One of the main supervision activities in 2021 consisted in monitoring compliance with the rules on FinTech players' access to payment accounts in credit institutions.

To ensure technical feasibility, credit institutions are required to create a technical access channel (dedicated interface) which FinTech players can use to offer their services. The specific technical requirements were defined by the technical standard for SCA (strong customer authentication)[1] & CSC (common and secure communication) , which came into force on 14 September 2019. Additionally, the EBA published an opinion in June 2020 on the obstacles in the dedicated interfaces and their elimination.

The Bank approved that EBA opinion and stated in a Communication dated 1 July 2020 that it was relying on this opinion for its interpretation of the ban on obstacles in the operation of the dedicated interfaces, and that it expected credit institutions to remove all hurdles from their dedicated interfaces by 31 December 2020.

The Bank has kept a close watch on this issue, but in the spring of 2021, on completing an in-depth analysis of the dedicated interfaces of each credit institution, it concluded that a number of obstacles still remained. That is why the Bank stipulated a deadline for the institutions concerned to remedy the situation. It is sure that most of these obstacles will be removed by mid-2022. It is also keeping a close eye on the interpretation of the current regulations on the subject, and providing additional technical information where necessary.

## 1.2 The digital euro

At the end of 2020, with its report on the digital euro, the ECB embarked on a detailed survey of the need to issue its own digital currency and how to proceed. In that context, experiments have already been conducted and a public consultation has been organised.

If the digital euro were to be launched, its aim would be to support the digitalisation of the European economy and to ensure its sovereignty in relation to foreign digital currencies or private means of payment. In view of the declining use of cash, at least in some Member States, this project could offer citizens an alternative way of ensuring access to central bank currency. That said, there is absolutely no question of discouraging or phasing out the use of cash. Nor is the aim to compete with the private sector. On the contrary, the idea is to promote cooperation with banks, payment institutions and other financial institutions.

The Bank is working with other euro area central banks on this project via the High-Level Task Force on Central Bank Digital Currency, a forum for discussing the main aspects relating to the design and characteristics of the digital euro. Indirect use is made of experts from within the Bank and outside. Various departments with experience in the sphere of cash and payments, macroeconomics, financial stability, technology and privacy protection, etc. are taking part in the project. To ensure that all stakeholders are involved in the project, the Bank keeps the private sector informed of its progress via the National Retail Payments Committee (NRPC – see section C.3.2).

## 1.3 Prudential treatment of crypto-asset exposures and draft European Regulation

Although the banks' crypto-asset exposures are currently limited, the expansion and continuing innovation of the market and services for these assets are arousing growing interest among banks. This could lead to new risks for financial stability and the banking system. In that context, on 10 June 2021, the BCBS launched a consultation on the prudential treatment of banks' crypto-asset exposures.

It proposes dividing these exposures into two groups according to certain characteristics of the crypto-assets:

- The first group concerns assets deemed eligible for treatment according to the existing Basel framework, subject to certain modifications and additional guidelines. That eligibility is determined on the basis of certain conditions relating in particular to the robustness of the stabilisation arrangements for stablecoins, and the legal framework of rights and obligations relating to the crypto-asset. This group is divided into two

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.

sub-groups: crypto-assets representing tokenised versions of traditional assets[1], and stablecoins.
- The second group comprises assets which do not meet all the eligibility conditions in the first group. They will be subject to a new, conservative prudential treatment.

Owing to the evolving nature of these assets, a second consultation will be published during 2022. This initiative does not concern central bank digital currencies (CBDCs).

It should also be noted that, in September 2020, the European Commission had published a proposal for a Regulation on Markets in Crypto Assets (MiCA), which forms part of its digital strategy. With this Regulation, the Commission aims to provide 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 (see section E.2.3 in the Report 2020).

### 1.4 Regulation and prudential expectations concerning the use of artificial intelligence

There have been various significant initiatives on the use of artificial intelligence.

On 21 April 2021, the European Commission published a proposal for a Regulation laying down harmonised rules on artificial intelligence (AI) in order to safeguard fundamental rights. It focuses the legislative effort on a small number of AI systems posing "high risks" for fundamental rights. In particular, this proposal provides for a preventive system which is based essentially on the establishment of compliance arrangements by suppliers of high-risk artificial intelligence systems and the supervision of those arrangements.

The proposal is not specific to the financial sector, though it does have a more tangible, immediate impact on lenders, as it considers that AI systems intended for assessing the solvency of individuals or to establish their credit rating are high-risk systems. Institutions deemed to be suppliers of that type of system will therefore be subject to additional obligations, such as the establishment of a risk management system, appropriate governance and data management practices, or human oversight.

AI system providers are covered by the draft Regulation if they develop an AI system or have an AI system developed in order to place it on the market or put it into service in their own name. However, there is an exception for AI systems put into service by small-scale providers and used exclusively by them.

Under the proposal, the Commission may, in the future, extend the list of high-risk systems to include other systems presenting a risk of negative consequences for fundamental rights, equivalent to or greater than the risk of negative consequences presented by the high-risk AI systems already identified. It is therefore possible that other systems such as certain specific systems used by insurers may ultimately be regarded as high-risk.

The EBA which, had already published a report in mid-January 2020 on the main trends in the use of big data and advanced analytics in the banking sector, has now concentrated on the use of machine learning for the purpose of the internal models used to calculate the regulatory capital for credit risk. Machine learning is used for various purposes in this context, such as validation, data quality improvement, or enhancing the model's predictive power. Thus, on 11 November 2021, the EBA published a consultation document on this type of use of machine learning. Among the problems associated with this type of use, the EBA mentions the interpretability and explainability of the results, complexity and governance, including knowledge and understanding of the model. The EBA proposes some recommendations in that connection.

### 1.5 FinTech survey and analysis for credit institutions

In 2017, the Bank launched a survey on FinTech and digitalisation covering a selection of banks and financial institutions. It provided a general picture of the impact of FinTech on the Belgian financial sector and facilitated the launch of a dialogue with market

1 The consultation document defines crypto-assets as "private digital assets that depend primarily on cryptography and distributed ledger or similar technology". Crypto-assets which represent tokenised versions of traditional assets are therefore those which use alternative means of recording the ownership of the traditional assets based on these technologies, rather than a central depository account.

players on various digital themes. The analysis of the survey responses was communicated to the participants and the public in 2018, together with a range of best practices concerning governance, organisation and monitoring in regard to FinTech and digitalisation.

Since that first survey, financial technologies and the resulting business models have continued to evolve, and new technology-based financial services have emerged. Customer preferences are also constantly changing, making the digital provision of banking services ever more important. That trend was further reinforced by COVID-19. Finally, some regulatory initiatives such as PSD 2 (see above) have since come fully into force. In 2020, the Bank therefore decided to conduct a new survey to update its knowledge of developments in the field, to gauge the response of institutions to the problems pinpointed, and to continue the dialogue with the sector.

To that end, in the second half of 2020, the Bank sent out a second structured questionnaire on the impact of FinTech, asking participants about a number of general environmental aspects relating to FinTech and digitalisation, recent and future developments in business models and financial technologies in each institution, projects relating to certain FinTech applications and their maturity, and finally, the overall strategic vision concerning FinTech and digitalisation. At the beginning of 2021, the responses were analysed and, in some cases, clarified by the institutions concerned. The results of that analysis were shared with the sector during 2021 and published separately[1]. In general, the survey revealed that the banks had taken account of a number of best practices regarding organisation and governance identified following the first analysis in 2017. Thus, most banks have now included profiles with knowledge of digital technology and IT in their management bodies, and have taken steps to adapt their organisation in order to encourage and facilitate innovation. Nonetheless, many of them are having difficulty attracting the necessary talent to support the digital initiatives. Most institutions have also defined a strategic vision regarding FinTech and digitalisation. However, key indicators of actual performance providing a clear view of how this vision is translated into reality are often lacking. In practice, that is reflected in significant variations between institutions in terms of digital performance and the development of new, innovative or digital applications. It is also evident that the smallest banks are often positioned as "followers". There is a risk that the business model of some banks may come under pressure, not only because of competition from new players such as BigTech, but also because the banks which are farthest advanced along the road to digitalisation and the integration of FinTech solutions will set the bar higher for all players in the sector by providing a more appropriate and/or more effective response to customers' wishes.

*The Bank sent out a new questionnaire to financial institutions on the impact of developments concerning FinTech/InsurTech*

## 1.6 InsurTech survey and analysis for insurance undertakings

In a world where digitalisation is occupying an ever more prominent position, new technologies will also have a great influence on the insurance sector and on insurers' business model. That will open the way to financial innovation, but it will also lead to the emergence of new risks. In that context, the Bank conducted an initial analysis on the scope and impact of digitalisation in the insurance sector on the basis of the data at its disposal.

It found that both insurers and InsurTech firms were actively contributing to innovation on the Belgian market, and that more or less all aspects of the value chain were concerned, even if the effects are mainly felt in the distribution or underwriting of insurance policies and claims management. The Bank likewise found that an array of technologies was already in use, such as digital platforms offering existing or new services on line, or services using robotic process automation. Innovative technologies such as artificial intelligence are also used to improve pricing. The analysis showed that this development primarily affected the non-life branches (such as motor and fire insurance) and to a lesser extent health insurance and credit insurance.

To develop this analysis further, the Bank sent out a new questionnaire to the insurance sector to obtain more information on insurers' vision and

1 See www.nbb.be/fr/articles/la-banque-nationale-publie-une-nouvelle-analyse-de-la-transformation-numerique-dans-le.

strategy regarding digitalisation, new technologies, and the costs and potential benefits of using these technologies.

## 2. Digital operational resilience

### 2.1 Cyber risks and IT risks

The COVID-19 pandemic was again the dominant feature of the year in 2021. The financial sector has therefore long since switched to large-scale remote working. While widespread working from home does reduce the health risks, it increases the cyber risks and IT risks unless it is accompanied by supplementary measures and checks. For instance, the resolution of incidents is hampered not only because there are fewer operators physically present but also because of the large number of business computers simultaneously connected remotely to institutions via the internet. Finally, cyber criminals are likewise taking advantage of the new opportunities available to them in the pandemic situation. Fortunately, thanks to precautions taken by the institutions, there were no really serious operational incidents during the year under review.

*Cyber attacks have become a daily occurrence worldwide in recent years*

In recent years, cyber attacks had already become a daily occurrence throughout the world. At the same time, the attackers are evidently continuing to refine the techniques and methods that they use, making some of the attacks ever more sophisticated, powerful and/or extensive. The number of targeted, long-lasting cyber attacks is therefore set to rise further in the future, as the financial sector remains logically one of the potential targets. The think tank Carnegie Endowment for International Peace[1] lists the cyber attacks targeting financial institutions worldwide. That document indicates the current situation regarding cyber threats facing the sector. In 2021, the listed attacks aimed, for example, to steal sensitive data, disrupt systems and initiate fraudulent transactions. Reported cases often included the use of ransomware or (crypto)malware, denial-of-service (DDoS) attacks, and the exploitation of institutions' vulnerabilities, particularly their supply chains, and/or staff credulity.

Insurance and reinsurance undertakings and groups are in a special position, being vulnerable to cyber risk on two fronts: as institutions, they are subject to cyber attacks, but they also feel the impact of attacks on their customers, either via explicit cover (affirmative cyber insurance), or via implicit cover (silent insurance or non-affirmative cyber insurance). With the growing number of cyber attacks during the pandemic and the public's greater awareness of the possibility of being targeted, the Bank expects the growth of this cyber insurance market to gather pace.

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

1 See Timeline of Cyber Incidents Involving Financial Institutions – Carnegie Endowment for International Peace.

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 encouraged to renew their sometimes very obsolescent IT architecture in a fairly short space of time, but the complexity of their IT environment makes it a major challenge to achieve that under properly controlled conditions. 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, at sectoral level, a small number of critical service providers present an ever-increasing concentration risk for the financial industry. The need for sufficiently extensive testing of software and recovery solutions to cover a range of 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.

## 2.2 Legislative guidelines and developments

In recent years, the Bank has made a substantial contribution to a regulatory framework designed to improve the control of cyber risks and IT risks. The prudential Circular on the Bank's expectations concerning the operational business continuity and security of systemically important institutions 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 auspices of the EBA, this resulted in the publication of the EBA guidelines for supervisory authorities on ICT risk assessment under the SREP, guidelines on outsourcing arrangements, and guidelines on ICT and security risk management. Under the aegis of EIOPA, a comparable regulatory framework was likewise set up for the insurance sector in the form of guidelines on outsourcing to cloud service providers and guidelines on ICT security and governance. These guidelines have meanwhile all become part of the Bank's supervision and policy framework. For payment systems and market infrastructures, the ECB's oversight expectations concerning cyber resilience are the benchmark. There have likewise been significant developments at global level. As stated previously in section B.1.2, in March 2021, the Basel Committee published new principles aimed at strengthening banks' operational resilience. Those principles are obviously highly relevant in a digital context. There is also a specific principle concerning ICT and cyber security.

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 ICT governance and risk management, ICT incident reporting and information-sharing, security tests and risks relating to ICT 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 legislative texts at European level and will probably also be closely involved in the subsequent development of technical standards.

## 2.3 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 2021, 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, it 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. In 2020, 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 methodology used and the benefits offered by these specific tests. Meanwhile, the TIBER-BE team also successfully conducts cross-border tests, in close and effective collaboration with other EU countries which have implemented the TIBER framework, and with the UK, which has developed a similar framework, called CBEST. Nevertheless, the TIBER-BE programme is coming to the end of its first cycle and the experience gained is being actively incorporated into the reference framework for a second cycle which will begin shortly.

The Bank is also paying closer attention to sectoral initiatives. For instance, the SSM regularly conducts transversal analyses on cyber- and IT-related subjects and cybernetic aspects. In 2021, for example, all significant banks and some less significant banks were again asked to complete a questionnaire which is to provide important data on IT aspects for the annual SREP and will permit cross-sectoral analyses. A large number of insurance undertakings, investment firms, payment institutions and electronic money institutions were also asked to provide such information for a similar purpose.

The Bank used another questionnaire to ask the entire insurance sector in Belgium about various aspects of cyber risk, and informed the firms of the results of its analysis, particularly those implying a lack of control on certain points (see box 12).

BOX 12

## Principal observations on the cyber risk questionnaire for the insurance sector

On the subject of cyber risk that companies in the insurance sector directly face, the Bank's analysis based on a questionnaire showed that:

- Cyber attacks most frequently target international and significant undertakings;
- International and significant undertakings understand the cyber risk better thanks to specific risk management frameworks and processes for collecting data and assessing the risk;
- Phishing e-mails are the most widely reported incidents in terms of frequency, but ransomware incidents are top of the list in the case of international undertakings.

The analysis also revealed that the cyber insurance market was still small in Belgium, with most undertakings not offering any cyber risk cover in 2019. Nevertheless, over the past four years, the Bank has seen this market expand.

Regarding cover for cyber risks, undertakings should be concerned about silent cyber risk (also known as non-affirmative exposure), i.e. the cyber risk implicitly covered by traditional non-life policies without insurers or reinsurers being aware of it. Insurance undertakings offering non-life cover that does not explicitly exclude cyber risk should revise their contracts in the future, because silent cyber risk cover can give rise to significant financial losses.

Qualitative methods are the commonest way of pricing cyber insurance, as quantitative approaches are difficult to implement owing to the lack of relevant data.

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 periodic 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 major incidents in the sector.

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