E. Digitalisation

Disruptive technologies and innovative business models are having an ever-increasing impact on the provision of financial services. In recent years, newcomers in the high-technology field have focused heavily on certain segments, such as payments, credit scoring and automated investment advice. With their innovative methods and platforms, these newcomers are responding directly to the changing needs of end users, such as convenience, immediate processing and cost efficiency. This chapter describes two trends in more detail: innovations in the payments sector resulting from the introduction of Open Banking, and global stablecoins (cryptocurrencies). The increasing digitalisation of financial services also means that a close watch must be kept on IT risks and cyber risks. The final section deals with developments in that area.

1. Open Banking

The second European Payment Services Directive (PSD2)[1], which was transposed into Belgian law by the Law of 11 March 2018, concerns innovations in the payments sector and requires account-servicing payment service providers (such as banks) to open up their online payment account infrastructure (Open Banking). This requirement enables payment initiation service providers and account information service providers (both banks, payment institutions and electronic money institutions) to enter the payment services market.

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.

2 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.

The opening up of this payment accounts infrastructure is accompanied by strict security requirements which must be respected by all the payment service providers concerned (banks, payment institutions and electronic money institutions). These security requirements are detailed in Commission Delegated Regulation (EU) 2018/389[2], which came into force on 14 September 2019.

The banking sector did not wait until these security requirements came into force before developing these new payment services on the Belgian market. Some Belgian banks already offer the option of using their own channels to consult payment accounts held with other Belgian banks and to initiate payment orders from those other payment accounts. In addition, in 2019, the Bank granted (or extended) licences for seven payment institutions and two electronic money institutions as payment initiation service providers and/or account information service providers.

The compulsory opening up of payment accounts by Belgian account-servicing payment service providers (principally banks) was brought about mainly by means of a dedicated interface developed by the banks concerned. At their request, and after having checked compliance with the legal requirements, the Bank exempted a number of these dedicated interfaces from the obligation to have a fallback mechanism in accordance with Delegated Regulation (EU) 2018/389. Many other banks will need to submit a similar exemption application to the Bank as soon as their dedicated interface meets the legal requirements on the subject. In view of the complexity and multiplicity of payment products offered by banks, it is taking more time than originally expected to develop an adequate dedicated interface.

The opening up of the payment accounts infrastructure is accompanied by strict security requirements

Regarding the application of strong customer authentication[1] for the secure initiation and execution of payments (both card payments and transfers), the EBA published an Opinion in June 2019 stipulating in detail the elements which can be used for strong customer authentication. However, it became apparent that the card industry needed a transitional arrangement for the use of payment cards in e-commerce settings. In accordance with the EBA Opinion on this topic, and in line with all other EU supervisory authorities, the Bank therefore published a Communication on 28 August 2019 acknowledging the challenges entailed in complying with strong customer authentication for Belgian payment card issuers and Belgian acquirers for these card transactions effected in e-commerce, and the need to cooperate with the parties concerned (payment service providers, payment card schemes, merchants and consumers associations, etc.) to agree a reasonable and acceptable migration plan – as quickly as possible after 14 September 2019 – enabling the sector to implement strong customer authentication for card payments in an e-commerce context. The Bank expects the sector to establish a migration plan that it is due to approve in the first part of 2020, so that this migration can take place by no later than 31 December 2020.

1 Strong customer authentication requires the use of at least two of the following three elements, which must be independent and confidential: an element that only the user knows (e.g. a PIN code), an element that only the user possesses (e.g. a payment card), and an element specific to the user (e.g. biometric data, such as a fingerprint).

2. Global stablecoins

One of the most striking trends in 2019 was the emergence of global stablecoins, backed by international consortia. Global stablecoin initiatives aim to set up an international financial infrastructure with a stable virtual currency and a wide user network. Price stability would be created by linking the virtual currency to assets with a fixed value, such as deposits and short-term government bonds. In addition, partners in international consortia wanting to launch these global stablecoins generally have a wide network of users (for example, Facebook as a partner in Libra) who are expected to support the use of the stablecoin as a means of payment. Price stability and network size are typical challenges for the first generation of cryptocurrencies such as Bitcoin.

Global stablecoins also reveal significant challenges for the current financial system. At present, the processing of international payments is often still inefficient and opaque. Moreover, financial inclusion is low in some parts of the world.

However, the introduction of global stablecoins may also entail major risks. Together with other international authorities the Bank is examining what those risks are, for example the use of global stablecoins for money-laundering, terrorist financing or tax evasion, or threats to privacy, competition and consumer protection (notably redeemability). There could also be significant implications for financial stability if the private consortium or one of its partners loses the confidence of the public.

It is also necessary to check whether the effectiveness of important macroeconomic instruments such as central bank monetary policy could be impaired if stablecoins gain ground.

When this Report went to press, it had not yet been possible to establish the extent to which the existing regulatory and prudential framework is adequate. Via international cooperation, the authorities are trying to obtain detailed information on the technical, operational and organisational design of global stablecoins. By an internationally coordinated approach, the authorities are endeavouring to avoid any regulatory arbitrage.

The Bank is actively involved in the continuous improvement of the payment systems used by central banks and plays an active part in the analyses on that subject in international working groups, such as the Committee on Payments and Market Infrastructures (CPMI).

3. Cyber risks and IT risks

3.1 Continuing rise in cyber threats and IT-related threats

Throughout the world, cyber attacks have become an everyday reality in recent years. At the same time, certain attackers are 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. Cyber criminals' ability to conceal the attack over long periods in certain cases permits misappropriation, intentional disclosure, and the modification or destruction of sensitive or critical financial data. In these circumstances, it is a challenge for financial institutions and infrastructures to provide adequate protection against the various attacks for their IT systems, services and data.

Together with other international authorities, the Bank is examining what risks global stablecoins may present

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 encouraged 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 a responsible way. There is likewise a high risk of growing dependence on third parties for IT services and other standardised IT system components. In particular, cloud solutions are increasingly being used, and for ever more important processes. That is also contributing to the fact that, throughout the sector, a small number of critical service providers present an ever-increasing concentration risk for the financial industry. The need for sufficiently representative testing of recovery solutions remains another key point for attention.

Assessing cyber risks and IT risks and promoting their control are therefore absolute priorities for the prudential supervision and oversight of financial institutions and FMIs, with European and international cooperation becoming ever more important. Individual institutions are strongly recommended to

continue stepping up their protective measures and efforts against cyber risks and IT risks. Due attention is also being paid to the sectoral control strategies being devised in Belgium and abroad. These two aspects are discussed in more detail in the sections below.

3.2 Guidelines

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[1] remains a key reference point. The Bank is also making an active contribution to establishing a European regulatory framework for the management of cyber risks and IT risks under the aegis of the EBA. For example, that work previously led to the publication of the EBA guidelines for supervisory authorities on the assessment of the ICT risk in the SREP for credit institutions and investment firms[2]. In 2019, that led to the guidelines on outsourcing[3], which have since become part of the Bank's policies, and to the guidelines on ICT and security risk management[4]. For insurers, the Bank is also contributing to the establishment of a similar regulatory framework under the auspices of EIOPA.

Throughout the world, cyber attacks have become an everyday reality in recent years

In regard to FMIs, in December 2019, the CPMI brought together experts from the sector to continue defining its strategy for reducing the risk of wholesale payments fraud. This led to the identification and formalisation of new measures which have proved effective. As co-chair of this CPMI working group, the Bank made a significant contribution. Like the other central banks belonging to the group, the Bank is working on the implementation of this strategy.

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

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

3 EBA Guidelines on outsourcing arrangements, February 2019.

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

3.3 Operational activities

Cyber risks and IT risks are a point for the Banks' attention in the course of its prudential supervision and oversight. In that sphere, it focuses on the security of individual financial institutions and FMIs and the confidence that they inspire, as well as on the sector as a whole.

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. In 2019, 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 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. All significant banks and some less significant banks were asked to complete an IT questionnaire which provides important information for the annual SREP, and also permits cross-sectoral analyses. A number of insurance undertakings were also asked to provide such information for a similar purpose.

In its role as the sectoral authority for application of the 2011 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. That is likewise the context in which the Bank organises 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 data system security, the Bank acts as the sectoral point of contact for incidents in the financial sector.

Finally, since the second half of 2018, the Bank has 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, and these tests are therefore conducted independently of its prudential supervision and oversight responsibilities. During the year under review, operational implementation of TIBER-BE continued.