F. Cross-sectoral aspects of prudential regulation and supervision

1. Introduction

In recent years, in its capacity as a supervisory authority, the Bank has played an active part in the work of the Financial Action Task Force (FATF) on combating money-laundering and terrorist financing. Section 2 of this chapter discusses Fourth Round Evaluation Report on Belgium. The report indicates that while Belgium has a robust system for the prevention of money-laundering and terrorist financing, it does not conform fully to the recommendations in some respects. In response to these findings, the Bank decided to conduct an in-depth review of the organisation of its supervisory powers on the subject.

During the year under review, technological progress also had a significant impact on the financial sector. Thus, the ever-growing importance of digitalisation led to the market entry of suppliers of software and applications supporting financial services, positioned alongside the traditional market players. Established players are responding to this trend by developing new applications or business models themselves, and/or by collaborating with these new entrants. This could entail new risks, and requires heightened vigilance, as explained in section 3.

Owing to the steady advance of digitalisation in the management of financial transactions and non-cash money and the importance of the internet in the financial sector, a detailed analysis of cyber risk management has become a priority for the prudential supervisor. Section 4 explains how the Bank addressed this need during the year under review, e.g. by issuing a Circular to systemic institutions clarifying its expectations regarding operational continuity and security, and taking an active part in the international efforts to improve cyber resilience.

2. Combating money-laundering

The Fourth Round Evaluation Report on Belgium was published on the website of the Financial Action Task Force (FATF) after being discussed at the plenary meeting of that international organisation on 26 February 2015. This report concludes that Belgium has the core elements of a sound anti-money-laundering and counter-terrorist financing (AML/CFT) regime, although some elements are not yet fully in line with the forty 2012 FATF Recommendations.

As regards the technical conformity of Belgium's provisions and mechanisms with those recommendations, it should be noted that the Belgian laws and regulations evaluated were still based on the previous version of the FATF recommendations. Consequently, the level of conformity found in Belgium in 2015 was lower than at the time of the third mutual evaluation by the FATF in 2005. However, that situation is temporary, and will be largely remedied by the transposition of the Fourth EU Anti-Money-Laundering Directive [1] and entry into force of the new EU Regulation [2] on information accompanying transfers of funds.

The evaluation of the effectiveness of the AML/CFT measures applied in Belgium likewise presents a mixed picture. While the effectiveness of these measures is assessed as substantial in regard to four of the eleven immediate outcomes defined by the new FATF evaluation methodology, it is assessed as moderate in regard to the other seven immediate outcomes. That result is attributable partly to the short time that Belgium was given to adapt to the new effectiveness requirements based on the evaluation methodology adopted by the FATF in February 2013.

In regard to the financial sector, a positive point is that the FATF found that companies in this sector have a good understanding of their prevention obligations and the risks to which they are exposed, and that the financial institutions generally seem to take appropriate preventive measures, including in high risk situations.

However, the report regrets that the supervision that the Bank exercises in this matter on the basis of assessment of the prudential risks does not take sufficiently clear and specific account of the assessment of the risks of money-laundering and terrorist financing associated with each of the supervised institutions. The available remote supervision tools need to be improved in that respect. The frequency of its on-site inspections also needs to be stepped up significantly in order to permit better supervision of the effectiveness of the measures applied by the financial institutions and to gain a more continuous insight into the risks. The FATF therefore recommends that the Bank should make more frequent use of its powers to impose sanctions where that is justified by the seriousness of the shortcomings found. In addition, the FATF considers that the Bank should do more to raise the awareness of the financial sector. The report emphasises that, in order to meet all these specific recommendations, the Bank needs to allocate more resources to AML/CFT supervision.

In view of the results of its evaluation, Belgium has to report annually to the plenary meeting of the FATF on the measures that will be taken to conform to the specific recommendations addressed to Belgium in the FATF report and to improve the level of technical conformity and effectiveness of its AML/CFT arrangements.

In the meantime, the above-mentioned Fourth EU Directive has been adopted and published, and preparations are

(1) Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money-laundering or terrorist financing, amending Regulation (EU) No. 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, Official Journal of the European Union, L141 of 5 June 2015.

(2) Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No. 1781/2006, Official Journal of the European Union, L141 of 5 June 2015.

under way for its transposition into Belgian law with the Bank's participation. The new European Regulation on information accompanying transfers of funds was published on the same day as the Directive and will apply from 26 June 2017, by which date the legal provisions transposing the Directive into national law must also be in force.

Taking account of the findings set out in the Mutual Evaluation Report and the FATF's recommendations addressed to the Bank, the latter also decided to conduct a fundamental review of the organisation of its AML/CFT supervision powers. The new set-up puts the emphasis on increased specialisation of the staff responsible for the remote monitoring of AML/CFT by bringing them together in a specialist group in charge of the prudential supervision on the subject. In addition, the staff assigned to this team are considerably specialised and their numbers are being increased. This team will carry out its duties in close cooperation with the inspection service, which will also have more resources allocated to on-site AML/CFT inspections. This reorganisation will make it possible to define and implement a supervisory approach specifically based on an assessment of the risks of money-laundering and terrorist financing to which each of the supervised financial institutions is exposed, so that the frequency and intensity of the supervision – both remote monitoring and on-site inspections – can be tailored more closely to those risks. Nevertheless, close links will also be maintained with the teams in charge of the general prudential supervision.

As regards its supervision tools, in 2015 the Bank continued with the process launched in 2013 of gradually developing and refining a periodic questionnaire on the prevention of money-laundering and terrorist financing which supervised financial institutions must complete each year. Thus, via a Circular dated 7 October 2015 the Bank sent out the new questionnaire which institutions must complete before the end of February 2016 on the basis of their situation as at 31 December 2015 (1). The main innovation in this third version of the annual questionnaire, introduced after consultation with the professional associations of the financial sector and the insurance sector, is that it now includes a new section designed to collect the quantitative data that will enable the Bank to improve its knowledge of each financial institution's classification of its customers and business relationships on the basis of its assessment of the associated money-laundering and terrorist financing risks. Quantitative data are also collected to provide a better understanding of the process for the production and analysis of internal reports on atypical transactions and the process for reporting suspicious transactions to the Financial Intelligence Processing Unit (CTIF-CFI).

The abridged questionnaire that small payment institutions and electronic money institutions have to complete each year was also supplemented with a section on the collection of the same type of quantitative data, but with due regard for the principle of proportionality (2).

As well as forming an extension of the process begun in 2013, this adjustment to the periodic questionnaire is also an initial, partial response to the recommendation made by the FATF to the Bank in the said Fourth Round Mutual Evaluation Report on Belgium, in order to refine and perfect its AML/CFT supervision instruments.

(1) Circular NBB_2015_26 of 7 October 2015 on the periodic questionnaire on the prevention of money-laundering and terrorist financing.
(2) Circular NBB_2015_27 of 7 October 2015 on the short-form periodic questionnaire on the prevention of money-laundering and terrorist financing.

3. FinTech : technological innovation in the financial sector

The central role of the processing and exchange of data in the provision of financial services has led to a high degree of digitalisation in the financial sector. FinTech is a generic term for firms that offer software and applications supporting the provision of financial services. The Bank notes that growing numbers of IT start-ups focus on the development of this type of software and applications, and position themselves alongside the traditional market players. It expects this digitalisation to have a significant impact on the financial sector, and therefore analyses the associated risks.

FinTech start-ups develop alternative approaches to the supply of financial products, e.g. new business models for consumer credit, national or international payments, and investment advice. Established players are responding to this trend by developing new business models and applications themselves, and/or by collaborating with these start-ups.

FinTech firms have the potential to bring about fundamental changes in specific segments of the financial sector, to improve the customer's experience and to cut costs.

Various techniques are used to improve the customer's experience. Expertise in data management and analysis is used to create accurate customer profiles, enabling the software and the products or services offered to be tailored to the customer's preferences. Particular attention focuses on the design of interfaces, with the emphasis on user-friendliness. In addition, the use of financial software on online platforms, such as online retailers, leads to simplification and, in many cases, faster processing of the transaction.

Alternative business models and processes generally combine ease of use with cost reduction. FinTech start-ups mainly opt for market segments offering large margins, and not necessarily a full range of products or services. By offering the software and applications worldwide, it is possible to reap economies of scale. Many FinTech solutions drive down the costs to the end user via extensive disintermediation. For example, in the case of consumer payments, there are solutions which are no longer based on correspondent banking relationships. In lending, banks can be circumvented by direct contact between the borrower and the lender via internet platforms (peer-to-peer finance model). These new models and processes may generate new risks (e.g. as regards compliance and regulation) which need to be analysed and monitored.

In contrast to the FinTech newcomers, existing financial institutions have developed an extensive framework of financial services systems supporting the full range of products. Financial institutions have the necessary expertise to respond to the compliance and regulation challenges. They have established strong networks with other financial institutions and have a relationship of trust with the end user. It takes substantial investment to set up such a framework.

Banks are aware of the large productivity gains achievable in the financial sector if they can link their own financial framework to new solutions from FinTech firms. The challenge for the banks lies in optimising and opening up this financial framework to prevent the FinTech solutions from evading their sphere of influence. In the resulting new ecosystem, end users will enjoy an extended range of innovative and reliable products and services.

4. Cyber risks

Digitalisation and the importance of the internet in the financial sector continue to grow, stimulated partly by innovative newcomers and the further rationalisation of the IT resources used. Financial institutions and FMIs are making ever-increasing use of specialised software/hardware components and service providers for the development and management of data systems (examples include the growing use of external clouds for data storage and processing).

Financial institutions and FMIs manage the information systems for the storage of non-cash money, the processing of financial transactions and the management of (confidential) financial customer data. These systems must be adequately protected against various forms of cybercrime, cyberespionage and cyberterrorism. An in-depth assessment of the management of cyber risk is among the top priorities of the prudential supervision and oversight of financial institutions and FMIs.

4.1 Sharp rise in cyber threats

Cyber risk analyses revealed various cyber threats. Major threats for the immediate future include the growing use of externally developed software/hardware components and external service providers, dependence on a small number of technologies, long-term, targeted attacks and the presence of unreliable insiders.

The use of externally developed software/hardware components and external service providers involves three cyber risks. Thus, the integrity of an FMI's infrastructure may be impaired if it is managed by an external service provider. That may occur in various ways, e.g. by the deliberate or involuntary installation of malware, the alteration and/or deletion of data, or changes to configurations. Moreover, compromised systems of service providers may create access to the systems of the financial institution or FMI. Finally, software/hardware components bought in by the institution may incorporate methods of circumventing the data system's authentication processes (back doors).

Recent events have shown that commonly used basic technologies may have significant defects which undermine the good protection of the system, e.g. via a leak in the cryptography (Heartbleed). These defects, which are not always known to the technology developers, are found in many different applications. Long and complicated processes for updating the technology lead to additional exposure. Security experts predict that cyber criminals will continue to invest in tracking down these defects.

The number of advanced persistent threats is also expected to rise. For example, if cyber criminals are able to keep the attacks hidden from the system managers, data may be extracted over a long period. The development and use of these techniques generally require advanced specialist knowledge, which means that only a small number of groups have the necessary skills. However, these techniques are currently offered on the black market in user-friendly applications, and are therefore available to a broader public.

Apart from external threats, organisations also face unreliable insiders. An unreliable insider is an organisation's employee, subcontractor or other partner who abuses his access to the organisation's data systems in order to damage the organisation. Possible abuse includes the intentional publication of internal documents, the alteration or destruction of confidential data, and the restricting or blocking of access to data systems and/or confidential data.

4.2 Guidance on cyber resilience

During the year under review, the Bank drew up a prudential Circular for systemic institutions, defining

the prudential expectations regarding operational business continuity and security with special attention to cyber resilience. That Circular came into force on 1 January 2016. Subjects covered include raising awareness of security in software development, the physical and logical segmentation of internal IT systems, the use of strong authentication solutions for privileged administrator access to critical or sensitive IT systems, and the periodic organisation of large-scale security tests in which independent experts check the effectiveness and quality of the security on the basis of realistic attack scenarios carried out in an ethical manner.

The Bank plays an active part in the CPMI-IOSCO working group for the development of guidance regarding cyber resilience for FMIs. In 2015, the working group published a consultative paper setting out five categories of measures for the management of cyber risks and three general components. The five categories of measures are: cyber governance, identification of cyber risks, protection against cyber attacks, detection of cyber incidents, limitation of the impact of cyber incidents, and recovery after cyber incidents. The three general components are continuous testing of data systems, awareness of developments in the organisation's environment, and continuous improvement of cyber security strategies on the basis of acquired insight. Investments in the various categories of measures are mutually complementary. This guidance supplements the CPMI-IOSCO principles for financial market infrastructures. It clarifies and supplements the governance requirements (principle 2), the framework for comprehensive risk management (principle 3), settlement finality (principle 8), operational risk management (principle 17) and the links between financial market infrastructures (principle 20).

4.3 Cyber risk analysis

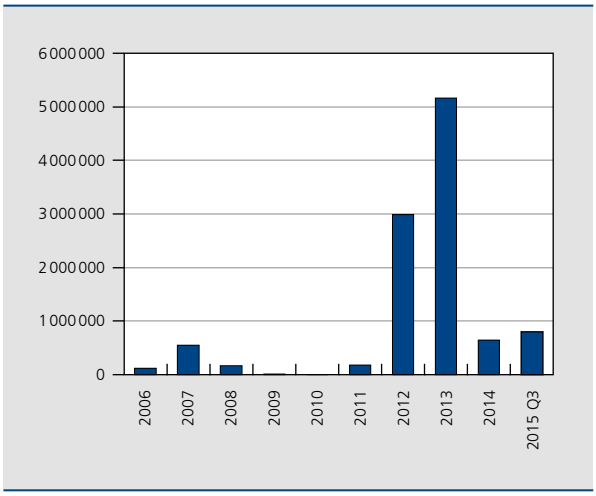
In 2015, both the prudential supervision and the oversight accorded particular importance to securing financial institutions and FMIs against cyber risks. European and international cooperation is becoming ever more important in that respect. Thus, in 2015, the SSM conducted a cross-sectoral review of cyber security covering the 130 largest banks and banking groups in Europe (the banks considered significant). On the basis of that review, other supervision measures were planned and carried out, including a number of targeted on-site inspections. In addition, a group of IT experts has been established in the SSM to improve the coordination, steering and monitoring of the supervision of the various IT risks and cyber risks specific to the sector as a whole. A new working group was also set up at the EBA for IT supervision, which will accord due attention to cyber risks as well as to the various IT risks. Another important platform for cooperation in combating cyber risks is the SecurePay Forum for the security of internet payments in Europe.

The close cooperation with entities such as Febelfin and the Federal Computer Crime Unit with a view to limiting e-banking fraud continued in the year under review. In this respect, it is worth noting that in 2015, as in 2014, instances of e-banking fraud remained stable at a low level in Belgium, notably as a result of the efforts made by financial institutions and following some successful arrests by the Belgian police and judiciary. As in 2013 and 2014, cases of e-banking fraud committed against private individuals in 2015 were due almost exclusively to fraud techniques whereby cyber criminals deceive users of e-banking into disclosing their personal security codes (usually after a telephone call or via a rogue website). In 2015, there were a few cases of fraud which specifically concerned professional e-banking channels and which used malware.

For the time being, the expansion of mobile banking services (via smartphone or tablet) has not led to any notable rise in the number of fraud cases in Belgium. The Bank is working with the sector to monitor the existing threats and the security solutions adopted by financial institutions.

CHART 10 ANNUAL FINANCIAL LOSS DUE TO E-BANKING FRAUD IN BELGIUM

(in €)



Source: NBB.