F. Cross-sectoral aspects of prudential regulation and supervision

As a prudential supervisory authority, the Bank has jurisdiction over a range of spheres which cover multiple sectors and are therefore not discussed in the sections of this Report on banking, insurance and financial market infrastructures. For instance, in recent years, the Bank has been actively involved in national and international work on combating money-laundering and terrorist financing. For that purpose, during the year under review, it adapted and reinforced its internal organisation in line with the recommendation by the Financial Action Task Force (FATF). Horizontal checks were also conducted on the implementation of financial sanctions against terrorists and terrorist organisations and – in the Panama Papers investigation – on the measures to prevent private tax arrangements and the laundering of money obtained by serious tax evasion.

During the year under review, the Bank created a new quality assurance function. Its task is to ensure that financial supervision conforms to the quality standards laid down by the SSM.

Technological progress in the financial sector has also led to the entry of new market players with a business model based on financial innovations. These FinTech players use new applications, processes or products and thus exert real influence on the existing financial markets and institutions, and on the provision of financial services in the broad sense. During 2016, an internal working group at the Bank observed their impact on existing business models and on prudential risks.

Cyber attacks are becoming increasingly sophisticated and causing ever more damage. The Bank paid particular attention to cyber risk management in financial institutions and individual FMIs, and in the sector as a whole. The efforts to improve cyber resilience were further intensified by specifically placing the emphasis on the management of that risk by financial players and on testing to assess the level of protection against attacks.

1. Measures to combat money-laundering and terrorist financing

1.1 Follow-up to the FATF mutual assessment of Belgium: continuing reorganisation of supervision

In order to respond adequately to the FATF's criticisms concerning the degree to which the Belgian laws and regulations conform to the new FATF standards, and taking account of the Belgian government's decision, following the terrorist attacks in Paris on 13 November 2015, to anticipate as far as possible the transposition of the Fourth European Directive on the prevention of the use of the financial system for the purposes of money-laundering or terrorist financing[1], the Bank together with the other public authorities concerned was closely involved in the working group responsible for drawing up, in the short time it was given, a pre-draft transposition law which respects all the requirements set out in the Directive, and at the same time brings the Belgian legislation as closely as possible into line with the 40 FATF recommendations.

(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, L 141 of 5 June 2015.

As announced in its 2015 Annual Report, in 2016, the Bank also made adjustments to its internal organisation in order to boost the effectiveness of supervision over the measures to combat money-laundering and terrorist financing (AML/CTF), supervision which it is responsible for exercising in the case of financial institutions under its jurisdiction. A specialist working group was thus set up to take charge of both the work on defining the prudential policy on the subject and the off-site supervision of the financial institutions, while maintaining close relations both with the services in charge of the general off-site supervision, and with the service responsible for on-site inspections. Apart from the fact that the centralisation of the off-site supervision work in a team of specialists in itself increases the attention that the Bank pays to performing this supervisory mission, the resources specifically allocated to that have already been increased substantially in 2016, both in the off-site supervision team and in the team responsible for on-site inspections. Further increases in resources are planned for 2017.

In consequence of all these measures, the Bank stepped up its contacts with financial institutions in the exercise of the off-site supervision, and the number of inspections increased considerably. Apart from the fact that these supervisory measures are aimed primarily at getting the institutions directly concerned to respond appropriately to the specific weaknesses identified in their case, the intensification of the AML/CTF checks – which will continue in 2017 and will be combined with the reform of the legal and regulatory framework as a result of the transposition of the 4th Directive – will also have the effect of making all financial institutions more aware of the vital need for effective internal AML/CFT mechanisms.

One of the Bank's objectives in this connection is, in particular, to ensure that the exercise of supervision on the subject is more systematically based on an analysis of the specific money-laundering and terrorist financing risks to which the supervised financial institutions are exposed. Measures have already been taken towards achieving that, notably on the basis of the responses by financial institutions to the annual questionnaire which they are required to complete[1], the annual reports by their AML/CFT officers, and the information available to the Bank in the exercise of its prudential supervision powers. However, this supervisory approach which the Bank will use must be consistent with the practices implemented in the other European Union Member States. The Bank therefore played an active part in drawing up the "guidelines", a task entrusted to the European supervisory authorities by the aforesaid 4th Directive. The recent publication of those guidelines[2] will enable the Bank to continue constructing its own risk analysis model while making sure that its practices tally with those of the other national authorities in Europe.

1.2 Horizontal checks concerning the freezing of terrorists' assets and the Panama Papers

Following the terrorist attacks on 13 November 2015 in France and on 22 March 2016 in Belgium, the Bank decided to conduct horizontal checks on the arrangements which all financial institutions have made in order to meet their obligations concerning implementation of the targeted financial sanctions against terrorists and terrorist organisations referred to in the Belgian and European lists on the freezing of assets and economic resources. Apart from the individual measures that resulted from these horizontal checks in order to remedy the defects found in some institutions, the Bank considered it particularly useful to make all those institutions more aware of their responsibilities in this regard by sending them a letter in which it sets out the lessons learnt from its checks, tries to clarify some aspects of the legal regime applicable which were not always properly understood, and expresses its expectations and recommendations with a view to improving the application of these financial sanctions[3].

In addition, following the publication of the Panama Papers in the press in April 2016, the Bank conducted horizontal checks on the implementation of both the measures to prevent special tax arrangements and the measures to prevent the laundering of money obtained by serious tax evasion (see box 14).

(1) The new version of the periodic questionnaire on the prevention of money-laundering and terrorist financing which financial institutions must complete between 1 January 2017 and 28 February 2017 on the basis of their situation as at 31 December 2016 was sent to them via the Circulars NBB_2016_42 and NBB_2016_43 of 26 October 2016.

(2) Joint Guidelines on the characteristics of a risk-based approach to anti-money-laundering and terrorist financing supervision, and the steps to be taken when conducting supervision on a risk-sensitive basis – The Risk-Based Supervision Guidelines", ESAs 2016 72, 16 November 2016.

(3) The horizontal letter of 6 December 2016 on the application of the financial sanctions regime (anti terrorist financing) is available on the website www.nbb.be.

Box 14 – The horizontal action relating to publication of the Panama Papers and the Governor's hearing before the Special Commission in the Chamber of Representatives

In the days following the April 2016 publication in the press of a list of off-shore schemes set up via a firm of Panamanian lawyers for the purpose of tax evasion or avoidance (the publication of the Panama Papers), and taking account of the possibility that some Belgian financial institutions may have been involved in some way in the devising or use of such special tax arrangements, the Bank conducted a horizontal action to ensure that the institutions under its jurisdiction respect their obligations concerning the prohibition and prevention of private arrangements having as their object or effect the favouring of tax evasion by their clients, and that they actually apply the mechanisms required to prevent the laundering of money derived, in particular, from serious tax evasion. First, the Bank required all these financial institutions to provide prompt answers to a number of questions intended to identify any institutions which may have helped their clients to set up shell companies in tax havens, and to find out whether their internal control systems had shed light on suspect operations connected with these special tax arrangements. Following analysis of the responses, interviews were held with the representatives of some financial institutions. Although this action did not cause the Bank to take significant measures, the information obtained from these horizontal checks will also be taken into account in the risk assessment forming the basis of the exercise of prudential supervision concerning measures to combat money-laundering and terrorist financing (see above).

At his hearing before the Special Commission on "international tax evasion/Panama Papers" in the Chamber of Representatives, the Governor of the Bank stressed the need for greater harmonisation, particularly in Europe, regarding the two specific tasks relating to the Panama Papers, namely combating special tax arrangements and defining the infringements underlying money-laundering, such as tax evasion. However, these two tasks are, by nature, territorial in character (link with tax rules for the prevention of special arrangements, and penal provisions in the case of the measures to combat money-laundering): the provisions on special arrangements are specific to Belgium and do not have a common European basis, while in regard to money-laundering, the definition of the underlying offences has yet to be harmonised. In the absence of European harmonisation, and in view of the territorial character of these provisions, the Bank as the supervisory authority has no power to take action against this type of arrangement in the case of a foreign subsidiary of a Belgian financial institution. Transposition of the 4th Directive by the EU Member States will be an important step leading all Member States to recognise serious tax evasion as an offence underlying money-laundering. In addition, groups of companies, including cross-border groups, will have to define a global anti money-laundering approach, applicable to all group entities.

In its report to the Special Commission, the Bank argued in favour of enhanced international cooperation between the various competent authorities in regard to money-laundering and terrorist financing. It also advocated setting up a "whistle-blower" scheme in the entities concerned, strengthening the compliance functions, and making the Law of 11 January 1993 on prevention of the use of the financial system for the purposes of money-laundering and terrorist financing applicable to firms advising on capital structure and industrial strategy, and offering advice and services in relation to mergers and acquisitions.

1.3 Due diligence in regard to asylum-seekers

On 12 April 2016, in view of the influx of asylum-seekers into Europe, the EBA published an Opinion[1] providing guidelines for financial institutions on how they can meet their legal obligations concerning ALM/TF without having to refuse asylum-seekers access to the financial system. These guidelines are based on the consideration that it is important for these asylum-seekers to have access to the financial system during their stay in Europe, not only because that access is essential for their integration into the life of society during their stay in Europe, but also to avoid a situation in which, if that access is denied, irregular financial services providers who endeavour to evade any supervision, particularly as regards ALM/TF, might find opportunities for developing illicit

(1) Opinion of the European Banking Authority on the application of customer due diligence measures to customers who are asylum-seekers from higher-risk third countries or territories, EBA-Op-2016-07,

activities by offering their services to these vulnerable people, further exacerbating the risks of money-laundering and terrorist financing confronting Europe.

The Bank forwarded this EBA Opinion to all financial institutions via a Circular[1] specifying the arrangements for applying in Belgium the principles promoted by the EBA, with reference to the Belgian laws and regulations as discussed in the Circular CBFA_2010_09 of 6 April 2010 on customer due diligence, the prevention of use of the financial system for the purposes of money-laundering and terrorist financing, and the prevention of the financing of the proliferation of weapons of mass destruction (coordinated version)[2].

2. Quality assurance

In 2016, the Bank set up a new quality assurance function which supplements its existing arsenal of tools for controlling the quality of its financial supervision activities. The aim of this function, which forms part of the second line of the Bank's three lines of defence model[3], is to give assurance that the Bank's financial supervision meets the relevant quality requirements, which concern the following four dimensions: "homogeneity and consistency", "respect for time limits", "content" and "conformity" with the regulations, and "best practices" which promote effective, efficient and rigorous supervision.

This new function's sphere of operations encompasses all the Bank's financial supervision activities, whether the Bank is acting as the resolution authority or as the authority in charge of the aspects of (macro and micro) prudential regulation and supervision, and whether it is exercising its responsibilities in the banking, insurance or financial market infrastructure sector. In particular, in the context of the SSM, the Bank's new quality assurance function collaborates actively with its counterparts at the ECB and in other national authorities in order to cover this specific sphere in the best possible way. In line with the cooperation arrangements set up within the SSM, the intention is that the quality assurance functions of the national authorities are directly responsible for guaranteeing the quality of the work done by their respective authority in regard to less significant credit institutions, and that they assist their counterpart at the ECB in its work concerning significant institutions.

The strategy adopted by this new function corresponds to the Bank's financial supervision strategy which forms part of a risk-based approach while ensuring, in particular, that the Bank meets the ECB's expectations in terms of quality assurance under the SSM.

In this context, the first quality assurance work is currently being carried out in the sphere of bank supervision, starting with less significant credit institutions. This project approach is among the tools available to the quality assurance function. Those tools also include the introduction and follow-up of instruments for continuously monitoring the quality of the financial supervision in general, or the conduct of ad hoc missions. The aim of the current quality assurance project is to identify, supplement (if necessary) and improve (if necessary) the processes, procedures and controls applied in the first line of defence, responsible for the supervision of less significant credit institutions. The project therefore aims to ensure that the set-up guarantees high-quality supervision in accordance with the four dimensions listed above.

3. FinTech

In recent years, the financial sector has been confronted by a multitude of innovations, driven by emerging technologies which are becoming ever more accessible. The entry into the market of many new players whose business model is based on these innovations is supported by sizeable growth in the amounts of venture capital invested in these newcomers and their financial technology. Changing consumer preferences further amplify this phenomenon. This trend is also known as the "FinTech revolution", FinTech being a generic term for all financial innovations leading to new applications, processes or products which have a significant impact on existing financial markets and institutions, and on the provision of financial services in the broad sense.

FinTech innovations are generally aimed at market segments where customers' expectations are not entirely fulfilled, whilst at the same time an attractive margin is achieved. In various segments of the financial sector, new FinTech players are appearing with an innovative business model such as crowdfunding, peer-to-peer loans, alternative means of transfers and international payments, robo

(1) Circular NBB_2016_32 of 12 July 2016 on the Opinion of the European Banking Authority (EBA) on the application of customer due diligence measures to customers who are asylum-seekers from higher-risk third countries (EBA-Op-2016-07)

(2) Circular CBFA_2010_09 of 6 April 2010 amended by Circular CBFA_2011_09 of 1 March 2011 on customer due diligence, the prevention of use of the financial system for the purposes of money-laundering and terrorist financing, and the prevention of the financing of the proliferation of weapons of mass destruction (coordinated version).

(3) The Bank's governance provides for a risk control model based on three lines of defence. It is thus the task of the Board of Directors and the operational management, as the first line of defence, to take on and manage the risks by implementing an appropriate and effective internal control system. The second line of defence defines the Bank's risk control framework, assists its implementation in the first line, and ensures that the latter implements the framework appropriately and effectively. Under this model, the internal audit acts as the third – independent – line of defence, applying a systematic and methodical approach in order to assess the internal control, risk management, and governance processes, and to recommend improvements.

advice, new electronic trading platforms, etc. These developments will undeniably have beneficial effects, such as an improved customer experience, lower transaction costs, and a wider range of services for customer segments previously not or under-served. At the same time, a new form of support services is emerging where FinTech players work together with existing market participants and offer certain operational processes which are more efficient, more secure, or better, such as cloud computing solutions, facilities for the electronic identification of customers, data analysis software that can be used to study customers' behaviour, and distributed ledger services which make it possible to eliminate intermediaries and conclude transactions in a more secure and efficient way.

The potentially disruptive impact of these FinTech developments on existing financial institutions has been widely debated in recent years and has led to numerous projections by supervisory authorities, regulators and financial institutions, among others. A first scenario, which is also the most extreme, results in the total disappearance of today's financial institutions, their place being taken by new digital players. In a second scenario, services are provided via FinTech players offering (alternative) financial products directly, resulting in disintermediation of financial institutions. Here we are thinking of initiatives taken in the financial sector by technology giants such as Google, Facebook, Apple, Amazon, Samsung, Alibaba, etc. In this scenario, existing financial institutions provide services to these new players, such as access to their infrastructure, product development, responsibility for compliance with the regulatory framework, etc. In a third scenario, financial institutions manage to develop business models themselves that meet the customers' expectations, possibly via a takeover or by integrating or collaborating with new players. They thus succeed in maintaining the customer relationship. At the current juncture, it is impossible to predict how quickly a given scenario will materialise and what its consequences will be. In practice, we shall probably see a combination of these various scenarios, and the outcome is likely to vary according to the market segment.

The FinTech revolution could also bring new risks, notably for the profitability of existing financial institutions which could possibly lose some lucrative activities to the newcomers, at a time when their profitability is already under pressure. Faced with these developments, financial institutions have to be on the alert so that they can rapidly incorporate useful innovations in their business model and adapt their strategy to those innovations. These changes also give rise to new operational risks, relating to increased dependence on IT systems and the expected growth of outsourcing to new players unfamiliar with the regulatory framework. Particular attention must be paid to protecting data and privacy, and to the reliability and scalability of these new technologies and applications. It is important to strike the right balance between customer convenience and containing operational risks. It is also essential to establish a clear management structure with well-defined roles and responsibilities. Moreover, new challenges are emerging, such as the detection of any errors in the algorithms used, customer identification in the case of remote transactions, and the detection of money-laundering schemes with the aid of new technologies. In a broader perspective, questions arise in the areas of consumer protection and personal data protection, since in the future financial services will increasingly be offered by firms with a non-financial background.

The Bank observes that a relatively small number of new players have so far applied for a licence for FinTech-related business models, whilst most existing players are working on improving customer experience through the development of mobile applications. In addition, initiatives are being taken to improve efficiency in the management of the IT architecture, including by means of cloud computing solutions. In many cases, it seems that the new players are working together with the traditional banks and do not aim to develop a full range of banking activities themselves. In the case of the FMIs, the Bank observes that they are in an exploratory phase, examining the extent to which FinTech applications would enable them to enhance the efficiency and effectiveness of existing processes. Both banks and FMIs are studying the potential advantages of "distributed ledger" technologies and data analysis. On the basis of an analysis of the general transaction data, banks will be able to develop a personalised offer for their customers and thus improve their services. In regard to the infrastructures' clients, the new technologies will offer solutions that make it easier to fulfil their compliance obligations. In addition, data analysis techniques will permit timely detection of suspect transaction patterns and thus minimise the impact of such fraud. By revising its Payment Services Directive (PSD2) [1], the European Union has opened the market to firms which give consumers and service providers access to information on bank accounts. The Bank finds that the new status of payment initiation service provider is attracting keen interest. These service providers act as a virtual bridge between the client and his internet bank account. They also indicate whether the client's account balance is sufficient and whether the underlying transaction can therefore be executed.

(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.

From the regulatory and supervisory angle, it is important that the right balance is struck, both for existing institutions and new players, between avoiding unnecessary hampering of innovation and controlling the risks. Points of attention here include the fact that FinTech puts pressure on the traditional revenue model, potentially jeopardising the stability of individual institutions and, by extension, the stability of the financial system. It is equally important that the new players have the necessary integrity and sufficient starting capital. It is also essential to ensure the stability and security of the IT systems and to take account of the "privacy" aspects when using the many linked databases (big data). At the end of 2015, the Bank set up an internal working group whose responsibilities include examining the future impact of FinTech on the business models of existing institutions and on prudential risks.

In the HLEG, the Bank also participates jointly with the law-makers in various initiatives aimed at adapting the regulatory framework to this new, changing financial environment. For example, in cooperation with the FSMA, the Bank began analysing the current regulatory framework in order to remove any unnecessary impediments to innovative business models. The Bank is also preparing a central contact point for FinTech initiatives, for both existing and new players. Via an active dialogue with market players, this central contact point will keep abreast of the fast-changing and sometimes complex innovations, and answer questions on regulations, supervision and licences. It is clear from the nature of the FinTech revolution that the response by the supervisory authorities must be coordinated and developed at EU level, or even in a pan-European perspective. The Bank is working with various international institutions on the development of regulations fit for purpose that take proper account of the prudential risks and guarantee the stability of the financial system, without restricting the chances and opportunities offered by the FinTech innovations. In that context, the Bank participates in various working groups dealing with such matters as the licensing arrangements applicable to FinTech players, the requirements concerning the outsourcing of activities, and the appropriateness of the existing prudential framework, taking account of the FinTech innovations.

4. Cyber risks

The financial sector has already been computerised to a great extent, and further digitalisation of its business processes is ongoing. There is also a very high degree of interconnection between the operational processes of the various financial players. Moreover, financial institutions are increasingly opting for business models that outsource IT services on the basis of operational or functional specialisation. This more advanced and diversified digitalisation of the access channels for the banks' retail customers is only one of the aspects which must be taken into account in analysing the operational risk in financial institutions and FMIs.

During the year under review, as in previous years, cyber risks were the focus of ever-increasing attention in the financial sector. Assessing and promoting the management of cyber risk is among the top priorities of the prudential supervision and oversight of financial institutions and FMIs. The sector was encouraged to continue reinforcing its measures and efforts to protect against cyber risks, taking account of the cyber risk management strategies being developed on an intersectoral basis in Belgium and abroad.

4.1 Continuing rise in cyber threats

Cyber attacks are becoming increasingly sophisticated and are causing ever more damage. The number of attacks compromising the integrity of IT systems and data is also rising. That is a cause for concern for the Bank as a prudential authority. In that sphere, it focuses primarily on the security of individual financial institutions and FMIs and of the sector as a whole, and on confidence in those institutions. Operational security and the robustness of services critical for the proper functioning of the sector are crucial here.

Cyber risk is tackled in two ways. First, institutions are required to hold capital to cover their operational risks, including cyber risks. Also, the operational security and robustness of the critical processes of financial institutions and FMIs are closely monitored, the availability and integrity of the IT systems being a key factor.

Cyber attacks may come from inside or outside the institution, and the attackers may have various motives, ranging from financial theft to espionage or geostrategic sabotage, and including terrorism. That makes it very difficult for financial infrastructures and institutions to ensure that their IT systems, data and services are perfectly protected against all types of attack. Since cyber threats are evolving very rapidly, the defensive capability of the institutions and FMIs must be more flexible than ever in responding to changing patterns of attacks. It is vital to have solutions for collecting information on potential threats, attackers, and types of attack. In order to protect themselves against cyber attacks compromising the integrity of IT systems and data, financial institutions need not only conventional continuity arrangements based on separate data centres, but also adequate recovery solutions.

4.2 Directives on cyber resilience

The prudential Circular on the Bank's expectations regarding the operational continuity and security of systemic institutions entered into force on 1 January 2016[1]. It focuses in particular on cyber resilience. In June 2016, the CPMI and the IOSCO published recommendations[2] on cyber resilience, applicable immediately to FMIs. The Bank will check whether the FMIs located in Belgium comply with those recommendations.

One of the main points for attention in this prudential Circular and in the guidelines on oversight is the management of cyber risks by financial players. Controlling cyber risks not only implies focusing on the technology, but also entails sufficient attention to in-house threats from employees or management. Financial players must make their staff aware of cyber risks so that they know how the risk can arise and how they should respond. The management bodies must have the necessary expertise and information to monitor cyber threats effectively and keep them within acceptable limits.

The two guidelines mentioned above likewise recommend that financial players conduct tests to assess their degree of protection against cyber threats. Those tests are increasingly sophisticated and in some jurisdictions they are based on specific frameworks comprising a harmonised test methodology. The Bank is watching over developments in this sphere to ensure that sound management practices are also introduced in Belgium, taking account of any European or international initiatives on the subject.

The Bank is also monitoring the progress made on this subject outside the financial sector. For instance, the G7 published guidelines on an adequate framework for controlling cyber risks, and various countries are setting up a national cyber strategy for their main sectors, in most cases including the financial sector.

4.3 Selected topics

SWIFT

The Bank is the lead overseer for SWIFT, and exercises that oversight jointly with the other G10 central banks. This year, particular attention was devoted to the cyber attack in which $ 81 million was stolen from the Central Bank of Bangladesh, and other cases reported in the press where financial institutions were the victims of fraudulent SWIFT messages. These attacks never threatened SWIFT's central processing systems, but the perpetrators exploited security defects in the financial institutions that use SWIFT. These attacks demonstrate how important it is for SWIFT's member financial institutions to have adequate cyber defences. To help its clients, SWIFT has introduced an extensive programme of support and advice, closely monitored by the G10 central banks responsible for overseeing SWIFT.

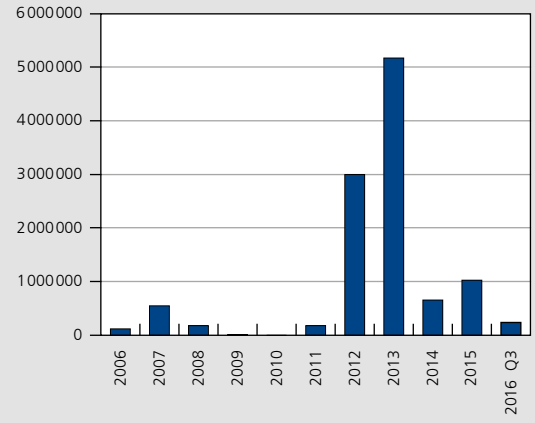
E-banking fraud and mobile banking fraud

The close cooperation initiated in recent years with Febelfin and the Federal Computer Crime Unit, among others, continued in 2016, with the aim of limiting e-banking fraud. Thanks to the efforts of the financial institutions and some successful interventions by the Belgian police and judiciary, the level of annual financial losses due to e-banking fraud has remained low over the past three years.

As in previous years, reported cases of e-banking fraud among consumers in 2016 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). The institutions analyse illicit transactions case by case and reimburse the victims, except in the case of gross negligence or fraudulent intent on the victim's part.

CHART 107 ANNUAL FINANCIAL LOSS CAUSED BY E-BANKING FRAUD IN BELGIUM

(in €)



Source: Febelfin.

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

(2) Guidance on cyber resilience for financial market infrastructures.