G. 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 Annual Report on banking, insurance and financial market infrastructures.

The year 2018 brought notable developments in the European legal framework concerning the prevention of money-laundering and terrorist financing plus, at national level, the entry into force of the new anti-money-laundering Law.

The quality assurance unit, which aims to ensure that the Bank's prudential supervision and resolution activities satisfy a number of quality requirements, continued that work.

On the subject of FinTech and digitisation, the Bank sent a questionnaire to a representative sample of institutions in the sectors comprising credit institutions, market infrastructures, payment institutions, electronic money institutions and insurance undertakings, in order to obtain a sectoral overview of the key trends and developments. One specific point for attention concerned the transposition of the second European Payment Services Directive (PSD2).

In view of the still growing cyber threats, the Bank actively contributed to the further development, at European level, of a regulatory framework for the management of cyber risks and recommendations on the subject. During the year under review, it also carried out several inspection assignments concerning cyber risk and set up a framework for ethical piracy. Finally, in collaboration with Febelfin, the Bank continued its work of mapping e-banking fraud.

As regards governance and the collaboration of auditors in prudential supervision, the year under review brought the preparation of a common approach by the Bank and the FSMA concerning the expertise of those responsible for the compliance function, publication of a communication on the renewal of auditors' accreditation, and a new "fit and proper" Circular. The Bank also took part in monitoring the recommendations of the Optima and Panama Papers commissions.

Finally, in 2018, the Bank made financial institutions aware of the risks that would result from a "hard Brexit", notably via contracts with British counterparties.

1. Prevention of money-laundering and terrorist financing

In regard to combating money-laundering and terrorist financing (AML/CFT) at European level, 2018 brought some notable changes in the legal framework and the emergence of new projects resulting from significant incidents which can be deemed to have revealed weaknesses in the existing legal framework or its implementation.

In Belgium, these developments are accompanied by the implications of the entry into force of the new anti-money-laundering Law of 18 September 2017[1]. During the past year, the Bank therefore paid particularly close attention to the effective implementation of that new Law.

1 Law of 18 September 2017 on the prevention of money-laundering and terrorist financing and limits on the use of cash.

1.1 Development and implementation of the European legal framework and new projects for the future

The 5th European Directive on AML/CFT[1] came into force on 9 July 2018. Instituted in response to the 2015 terrorist attacks in Europe, this Directive aims mainly to strengthen the European legal framework and that of the Member States in such matters as the vigilance measures applicable in regard to electronic money or high-risk countries, and the transparency of companies and legal structures, in particular by clarifying the scope of the concept of "actual beneficial owners" of trusts and similar legal arrangements. It introduces an obligation on the Member States to compile a list of prominent public functions, as the people entrusted with those functions become "politically exposed persons" requiring the exercise of greater vigilance[2]. It also requires Member States to make operators in virtual currencies subject to obligations preventing money-laundering and terrorist financing (AML/CFT) and to supervision on compliance with those obligations. In addition, the new directive aims to improve the functioning of national financial intelligence units and their mutual cooperation, and the functioning and interconnection of national registers of the actual beneficial owners of companies and legal structures. It likewise introduces a new obligation on Member States to set up a central register or mechanism permitting identification of the holders of bank accounts, payment accounts and

1 Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money-laundering or terrorist financing and amending Directives 2009/138/EC and 2013/36/EU (OJEU of 19 June 2018).

2 While some categories of politically exposed persons, such as heads of State, heads of government, ministers and so on are unequivocal, other categories, such as senior officers in the armed forces, members of the administrative, management or supervisory bodies of public enterprises, etc., may give rise to differing interpretations and be clarified by compiling such a list.

safe-deposit boxes. Finally, the 5th directive also includes various provisions to facilitate and intensify cooperation between the competent national supervisory authorities concerning AML/CFT, and with the prudential supervisory authorities, including the ECB acting under the SSM.

As this 5th Anti-Money-Laundering Directive has to be transposed into the national laws of the Member States by 10 January 2020, the Bank is taking part in the working group coordinated by FPS Finance – Treasury – which is in charge of drawing up the technical aspects of a preliminary draft transposition Law. The Bank will also put forward, in this connection, legislative provisions which properly clarify and reinforce the cooperation obligations of the national supervisory authorities in regard to AML/CFT, with a view to making that supervision more effective.

In factual terms, there have been a number of incidents in Europe recently which appear to reveal weaknesses in the implementation of the European legal framework on AML/CFT and its supervision in certain EU Member States. In view of these events, the European Commission published a communication [1] on 12 September 2018 listing the legislative and non-legislative measures which it recommends reinforcing in the short term both prudential supervision of banks and their supervision in regard to AML/CFT, as well as its ideas for the longer term.

As a short-term legislative measure, the Commission says that it wishes to remove all the legal obstacles to the exchange of information between prudential supervision authorities and the authorities supervising the AML/CFT of banks by amending the Capital Requirements Directive [2]. It also states that it wishes to supplement the current review of the founding regulations of the three European supervisory authorities [3] with additional amending provisions on their roles in regard to AML/CFT. These additional changes aim primarily to centralise powers relating to AML/CFT in the EBA, including in sectors of activity which come under EIOPA or ESMA. They are then meant to clarify the content of EBA's tasks in this area and strengthen the legal tools provided for that purpose. Among other things, the Commission envisages obliging the EBA to inform the European Parliament, the Council and the Commission of any serious unresolved shortcomings which it identifies, for instance in its peer reviews, and enabling the EBA to issue injunctions to both national supervisory authorities and financial institutions. Finally, in the short term the Commission wishes to give the EBA a central role in cooperation with the authorities of third countries.

On the subject of short-term non-legislative measures, the Commission encourages the European supervisory authorities, and especially the EBA, to make use of their existing powers. That includes drawing up "common guidelines" and the implementation of peer reviews and procedures for breaches of European law, both in order to ensure that the authorities in charge of the prudential supervision of banks take due account of the AML/CFT risks, even if those authorities do not simultaneously hold specific responsibilities for supervising AML/CFT, and to reinforce the Europe-wide effectiveness and convergence of the AML/CFT supervision exercised by the national authorities. The Commission likewise encourages the ECB to meet the deadline for concluding the agreement with the AML/CFT supervisory authorities required by the 5th Directive for organising their cooperation, and to clarify the arrangements for taking account of AML/CFT risks in the exercise of its supervisory powers.

Following a number of recent incidents in Europe, the European Commission published a series of measures aimed at strengthening supervision in order to combat money-laundering and terrorist financing

1 Communication from the Commission to the European Parliament, the European Council, the European Central Bank, the Economic and Social Committee and the Committee of the Regions strengthening the Union framework for prudential and anti-money-laundering supervision for financial institutions, 12 September 2018, COM (2018) 645 final.

2 Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC.

3 Regulation (EU) No. 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No. 716/2009/EC and repealing Commission Decision 2009/78/EC; Regulation (EU) No. 1094/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Insurance and Occupational Pensions Authority), amending Decision No. 716/2009/EC and repealing Commission Decision 2009/79/EC; and Regulation (EU) No. 1095/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Securities and Markets Authority), amending Decision No. 716/2009/EC and repealing Commission Decision 2009/77/EC.

In the longer term, the Commission announces that it will explore the potential for further reforms which could include replacement of the current Directive specifying the minimum degree of harmonisation in regard to AML/CFT with an EU Regulation directly applicable in the legal systems of the Member States, which would achieve full harmonisation of the national laws on the subject, and the creation or designation of a European authority centralising the responsibility for exercising supervision over AML/CFT.

Since the publication of this particularly important Communication by the European Commission, the Bank has played an active and constructive part in the technical discussions on the short-term legislative measures referred to above. Convinced of the need to produce a strong and effective European response to the recent incidents, the Bank is particularly careful in this context to ensure the high technical quality of the intended amendments to European legislation, and to maintain a proper balance between provisions specifically relating to AML/CFT supervision and those relating to prudential supervision.

It should be noted that, once these new provisions have been adopted and are in force, they could have a significant direct impact on the responsibilities of the Bank as both a national supervisory authority for AML/CFT and a prudential supervisory authority.

On 4 December 2018, responding to the same events as the European Commission, the European Council also published its Conclusions[1] on an Anti-Money-Laundering Action Plan, which sets out the measures which it intends to see implemented without delay both by the European Commission and the European authorities, and by the Member States and their competent national authorities, in order to rectify the shortcomings found.

1.2 Implementation of the Law on the prevention of money-laundering of 18 September 2017

Communication to financial institutions of their AML/CFT obligations

Following entry into force of the Anti-Money-Laundering Law of 18 September 2017, the Bank considered that, in order to ensure effective application of the Law, it needed an efficient communication instrument enabling it to provide financial institutions with complete, easy and regularly updated information, so that they would know and understand in detail all the legal and regulatory obligations to which they are subject in that respect. For that purpose, the Bank created a new section on its website, gathering together all the relevant texts on AML/CFT (Law, Regulations, preparatory work, European and international guidelines, etc.), and arranging them by subject in order to facilitate searches. This section can also be used to address to the financial institutions the recommendations and comments that the Bank deems necessary for the correct and effective application of the provisions of the law and regulation on the prevention of money-laundering.

After having placed the structure of the new website section and all the reference documents on line at the beginning of 2018, the Bank steadily enhanced it by adding its comments and recommendations in stages, subject by subject, after having first submitted its plans to the financial sector's professional associations for consultation. At the end of 2018, this website section thus contained all the recommendations which the Bank considered useful for all relevant aspects of the subject. There are alert mechanisms for informing financial institutions whenever significant changes are made to the website. It is also possible to consult earlier versions of the website. At a future stage, the Bank will also publish this website section in English.

In the future, the Bank will update this website regularly whenever it considers that necessary, notably to take account of changes in the standards and recommendations of the competent international bodies concerning AML/CFT, the European and national legal and regulatory framework and the interpretation of the applicable rules, etc.

Risk-based supervision methodology

Since the Bank is legally required to apply a risk-based approach in exercising its supervisory powers, it has to implement a supervision methodology in accordance with the common guidelines on

1 Anti-Money-Laundering Action Plan – Council Conclusions, 4 December 2018.

risk-based supervision, adopted on 7 April 2017 by the European supervisory authorities[1] and which the Bank stated that it would respect.

For that purpose, and on the basis of the experience gained in previous years, the Bank collects the summarised initial data that it needs concerning the inherent AML/CFT risks confronting each financial institution, the apparent degree to which its AML/CFT mechanisms conform to the legal and regulatory obligations, and the apparent effectiveness of those mechanisms by means of the periodic questionnaire, the 2018 version of which was produced on a sectoral basis[2]. In addition, in 2018, the Bank acquired supplementary IT tools giving it the benefit of an automated preliminary analysis of the responses to the periodic questionnaire submitted online by each financial institution, and also enabling it to take account of all the available information, including the result of the earlier off-site supervision and on-site inspections, the prudential information and the information obtained from accredited auditors or reliable external sources, in order to allocate an appropriate risk profile to each financial institution.

That risk profile determines the level of priority, frequency and intensity of the off-site supervision. Depending on the case, the checks may include detailed examination of the organisation charts, policies and internal procedures of the financial institution concerned, the collection and analysis of more detailed information from the institution, examination of internal audit reports and the way that they have been followed up, meetings with the AML/CFT officer and the senior director responsible, etc. Where appropriate, visits to the premises may be arranged in order to enable the supervision team to examine the situation in more detail, though these on-site visits do not follow the audit methodology applied to on-site inspections. Off-site supervision also includes monitoring the action plans produced by financial institutions following previous on-site inspections. These off-site supervisory actions are intended to determine the measures that the financial institution concerned must adopt and implement within a reasonable period in order to rectify the weaknesses identified. It may, if necessary, result in recourse to the constraint powers granted to the Bank by the Anti-Money-Laundering Law of 18 September 2017, such as setting deadlines for rectification, the imposition of penalties, ordering the replacement of directors, suspension of activities, etc.

The risk profile assigned to financial institutions taking account of the results of previous checks also serves as a basis for determining the priorities for on-site inspections concerning AML/CFT, and the subjects which those inspections will cover.

The Bank is continuing to strengthen its risk-based supervision tools

Checks on the effective implementation of the new legal and regulatory provisions

Since the entry into force of the Anti-Money-Laundering Law of 18 September 2017, the Bank has had to ensure that financial institutions subject to its statutory supervisory powers take the necessary action, within a reasonable time, to comply fully and effectively with their new legal and regulatory obligations. The most crucial of those is the obligation to conduct an overall assessment of the AML/CFT risks as the basis for their internal AML/CFT procedures and policies. The Bank therefore instituted checks whereby it requested all financial institutions under its jurisdiction to conduct such an overall risk assessment without delay, together with a systematic analysis of the weaknesses of their internal AML/CFT mechanisms in regard to both their new legal and regulatory obligations and the risks which they identified, and to produce an action plan for remedying those weaknesses within a reasonable period of time[3].

The Bank asked them to submit an interim report on this work by the end of March 2018, in order to ensure that the work had actually been started, followed in mid-July 2018 by a final report summarising the conclusions of their risk analysis, their analysis of the weaknesses, and their action plan for remedying them.

1 "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, 7 April 2017.

2 Circular NBB_2018_01 of 15 January 2018 / Periodic questionnaire on the prevention of money laundering and terrorist financing.

3 Circular NBB_2018_02 of 24 January 2018 / Global risk assessment concerning anti-money-laundering and terrorist financing.

The Bank incorporates this information in its risk-based supervision process as described above, giving priority to the examination of information supplied by financial institutions to which it has assigned a high risk profile. As well as continuing these checks in 2019, the Bank drew the financial institutions' attention to the fact that this work must be repeated when necessary to adjust their internal AML/CFT mechanisms in line with changes in the risks to which they are exposed.

Specific checks on funds transmission

In 2018, in view of the high risks specifically linked to the transmission of funds involving the substantial use of cash, the Bank completed the horizontal checks launched in 2017 and comprising the examination of a sample of transactions effected by agents of the main Belgian or foreign payment institutions (money remitters) operating in Belgian territory. For the purpose of these checks, the Bank first sent each of the payment institutions concerned individual recommendations on rectifying the weaknesses identified.

However, on the basis of all the analyses conducted and the additional information received, the Bank also found that certain shortcomings are common in these institutions' control procedures and systems. The points for attention identified essentially concern the supervision of agents, coding errors, vigilance over transactions between Belgian counterparties, situations which may reveal fragmentation of transactions, and finally, the need for exclusive management by the compliance function of requests for information and alerts.

The Bank therefore considered it necessary to publish a Communication[1] notifying the entire sector of the general lessons derived from these horizontal checks, while explicitly stressing the importance of rigorous compliance with the obligations under the legal and regulatory AML/CFT framework, and adherence to the internal policies and procedures established within payment institutions.

1 Communication NBB_2018_21 of 20 June 2018 / Horizontal supervisory analysis comprising examination of a sample of transactions concluded by agents linked to various payment institutions.

AML/CFT checks on the occasion of new applications for authorisation or registration of entities subject to the Anti-Money-Laundering Law of 18 September 2017

In processing applications for the authorisation of new financial institutions and the registration of new branches or other forms of establishment on Belgian territory which are subject to the Anti-Money-Laundering Law of 18 September 2017 and the Bank's supervisory jurisdiction, the Bank ensures that these entities will comply fully with their obligations on this matter, notably as regards their governance and organisational arrangements, and their policies, procedures and internal controls, on the basis of an appropriate overall risk analysis.

A particularly large number of applications of this type were submitted in 2018, notably in view of the United Kingdom's imminent departure from the European Union and the decision of many financial institutions based there to relocate to EU territory. This particularly concerns the electronic money and payment institutions sector, but also the credit institutions sector. In regard to these applications, the Bank pays special attention to obtaining the assurance that the decision-making centre for performance of the AML/CFT function is actually located in the Belgian entity and that the organisational measures implemented permit effective performance of that function.

The processing of these applications had a very significant impact on the allocation of the human resources which the Bank assigns to the performance of its supervisory powers relating to AML/CFT.

2. Quality assurance

The quality assurance unit continued the work initiated in 2016, which aims to ensure that the Bank's prudential supervision and resolution activities (in both the national and the international context) meet the specified quality requirements.

More than half of the work done concerned banking supervision, and was centred on three main aspects: finalisation of a quality assurance mission which aimed to assess whether the governance, organisation and functioning set up by the Bank in the context of the SSM enable it to perform

adequately its role as a national competent authority in relation to the ECB ; the Bank's role as the NBB single point of contact for ECB in terms of quality and as contributor to its quality assurance work under the SSM ; and continuation of the work on improving the quality of the processes, procedures and checks applied within the operational services responsible for the supervision of less significant institutions (LSIs).

The quality assurance unit also had to intervene occasionally, as a facilitator, coordinator or adviser, in a whole range of cross-sectoral issues, i.e. dealing with subjects which concern more than one prudential supervision service at a time. These actions were initiated by the quality assurance unit or in response to a request from the Bank's management. For example, the quality assurance unit played a key role in 2018 in ensuring that the cross-sectoral recommendations of the Internal Audit addressed to the prudential supervision services are properly implemented.

The network of quality assurance correspondents from the Bank's operational supervision and resolution services continued its work. That relates both to the regular, structured exchange of information on quality, and to consultation on the definition of initiatives to improve the quality of their activities. This led to the continuing implementation within those services of the quality targets defined to ensure that supervision would be effective, efficient and rigorous.

3. FinTech

In recent years, driven by technological innovations and changing consumer preferences, the financial sector has become increasingly digitalised, with the introduction of numerous new applications, processes and products. Digital transformation and FinTech [1] are closely linked concepts and are characterised by both the arrival on the market of new, innovative service providers and initiatives of existing institutions aiming to improve their organisation, their provision of services and their product range with the support of technological innovations.

The Bank recognises the importance of these developments and has therefore taken various measures to establish a dialogue on these issues with both new and established market players. In that context, the Bank set up a central contact point (FinTech single point of contact), in close coordination with the FSMA, to address FinTech-related questions [2].

The Bank made the financial sector aware of the challenges concerning FinTech and digitisation

In view of the potential influence of new technologies on the financial market, the Bank also aimed to develop a sectoral overview of significant trends and developments concerning Fintech and digitisation in the Belgian financial landscape. Therefore the Bank sent a structured survey in the second half of 2017 to a representative selection of institutions in the sector comprising credit institutions, market infrastructures, payment institutions, electronic money institutions and insurance undertakings.

The survey aimed to assess the outlook and general observations of the industry on FinTech, the prospects for certain business models and specific technologies, the practical strategy pursued by institutions with regard to Fintech, and observations or comments related to regulation and supervisory practices. The horizontal survey also aimed to obtain an idea of the stance of the various players with regard to FinTech, the potential impact of these developments on their current business model, and the measures they expect to take to deal with this trend.

3.1 Survey for credit institutions

The responses by credit institutions showed, *inter alia,* that they first of all intend to modernise in order to remain relevant in the future. Banks also consider it relatively plausible that financial services will become increasingly modular and that banks can retain sufficient business, while a large number of new, specialist companies take over certain specific activities, notably

1 The Financial Stability Board (FSB) defines the FinTech concept as technology-enabled innovation in financial services that could result in new business models, applications, processes or products with an associated material effect on financial markets and institutions and the provision of financial services.Circular NBB_2018_02 of 24 January 2018 /Global risk assessment concerning anti-money-laundering and terrorist financing.

2 The central FinTech contact point may be found at https://www.nbb.be/fr/supervision-financiere/generalites/point-de-contact-fintech.

by offering them directly on the platforms of banks and technology companies.

The banks are of the opinion that their main strength lies in their established client portfolio, their customer knowledge, and the confidence that the customers have in them. Furthermore, they believe they also have an advantage over the new financial institutions in terms of knowledge and experience, both on the level of the oftencomplex regulations and on the level of risk management.

On the other hand, the Belgian banking sector expressed its concerns about its often aged IT infrastructure, which may lead to higher operating costs, inefficient processes, or an increase in the associated risks, and problems in implementing innovative business models. In addition, the survey responses highlighted that a number of banks have no clear strategy on FinTech and digitisation, which means that they have no clear view on the situation and often demonstrate reticent behaviour. In each market segment there were clear examples of these banks with no innovation-strategy, while some of their direct competitors were clearly gaining a competitive advantage through their continued efforts in this matter. The survey also demonstrated that banks of a more modest size rather position themselves as "follower", and refer to the fact that, in terms of operational and financial capacity, they are less able to experiment, and that big banks are more attractive to FinTech entities for developing partnerships.

With regard to the impact of FinTech, the banks highlighted cyber risks in particular, alongside the risks related to their profitability and strategy, and the risk that their role will may decline if customers conclude transactions directly with investors, thereby by-passing their function as intermediary.

At the end of 2018, the Bank published the results of this analysis on its website[1] and drawing attention to a number of good practices in this context. An essential part of these recommendations refers to the necessity for designing, implementating and managing a clear strategy, in which the role and participation of the board of directors proves to be a key success factor. The banks must also be sufficiently aware that, in certain cases, FinTech and digitisation projects are necessary to maintain their current market position and business model, and to continue to meet the customers' changing needs.

1 Analysis of the impact of fintech and digitalisation on the Belgian banking sector and supervision, NBB, 22 November 2018 (https://www.nbb.be/fr/articles/analyse-de-limpact-de-fintech-et-de-la-numerisation-sur-le-secteur-et-le-controle-bancaires)

3.2 Survey for payment institutions, electronic money institutions and financial market infrastructures

The survey responses from payment institutions, electronic money institutions and financial market infrastructures highlighted that, despite the introduction of new technologies and innovation in the sector, most of the clearing and settlement activities still take place on the existing payments and market infrastructures. The market infrastructures and payment institutions that took part in the survey noted that new developments in the field are aimed mainly at optimising customer relationships (front-end). Furthermore, the survey showed that the respondents observe a higher level of competition in the payments market, that puts more pressure on the margins of existing players. The sector is of the opinion that this trend is driven on the one hand by the need to improve the customer experience, and on the other hand by the arrival of the "Open Banking" concept (see section G. 4) in the market, which enables new third parties to enter the market. Finally, most of the respondents also indicated that they were closely monitoring the developments with regards to the digitisation of the financial sector.

3.3 Survey for insurance undertakings

The questionnaire the Bank sent out to insurance undertakings aimed to provide some idea of what the various existing players are thinking and to ascertain their views on the impact of InsurTech on the European and Belgian insurance markets and the main legal obstacles that could prevent Belgian insurers from implementing their strategy in that regard.

The responses that, in the short term, InsurTech[1] is seen more as an opportunity for improving the services of insurers than as an immediate threat. Insurers are preparing for the arrival of these new technologies, and the potential impact on their business model or internal organisation is generally being discussed at the level of the board of directors or the executive board. The independent audit functions are also consulted during the decision-making process, and special internal groups are being set up. The sector's primary concerns relate more to the changes needed for their business model than to the entry in the market of new market players. Insurers are also of the opinion that, in some cases, the current legislation limits the application of new technologies on consumer protection grounds.

In the medium term, the internal processes of insurers can be improved, for instance by enhancing their IT organisation, by creating new departments (e.g. data management), or by stepping up the use of robots for recurrent tasks. The claims assessment process and fraud prevention will also be improved, which in turn will have an impact on the contract premiums. Insurers expect more personalised risk coverage and hence a decline in risk mutualisation.

In the longer term, insurers generally consider that, over the next ten years, digitisation and InsurTech will play a vital role on the market in terms of product distribution, customer service, and even product design, and in risk assessment and pricing. In some cases, the changes to the way in which products are developed, priced or marketed will limit the insurers' role to that of a "risk bearer".

4. Open Banking

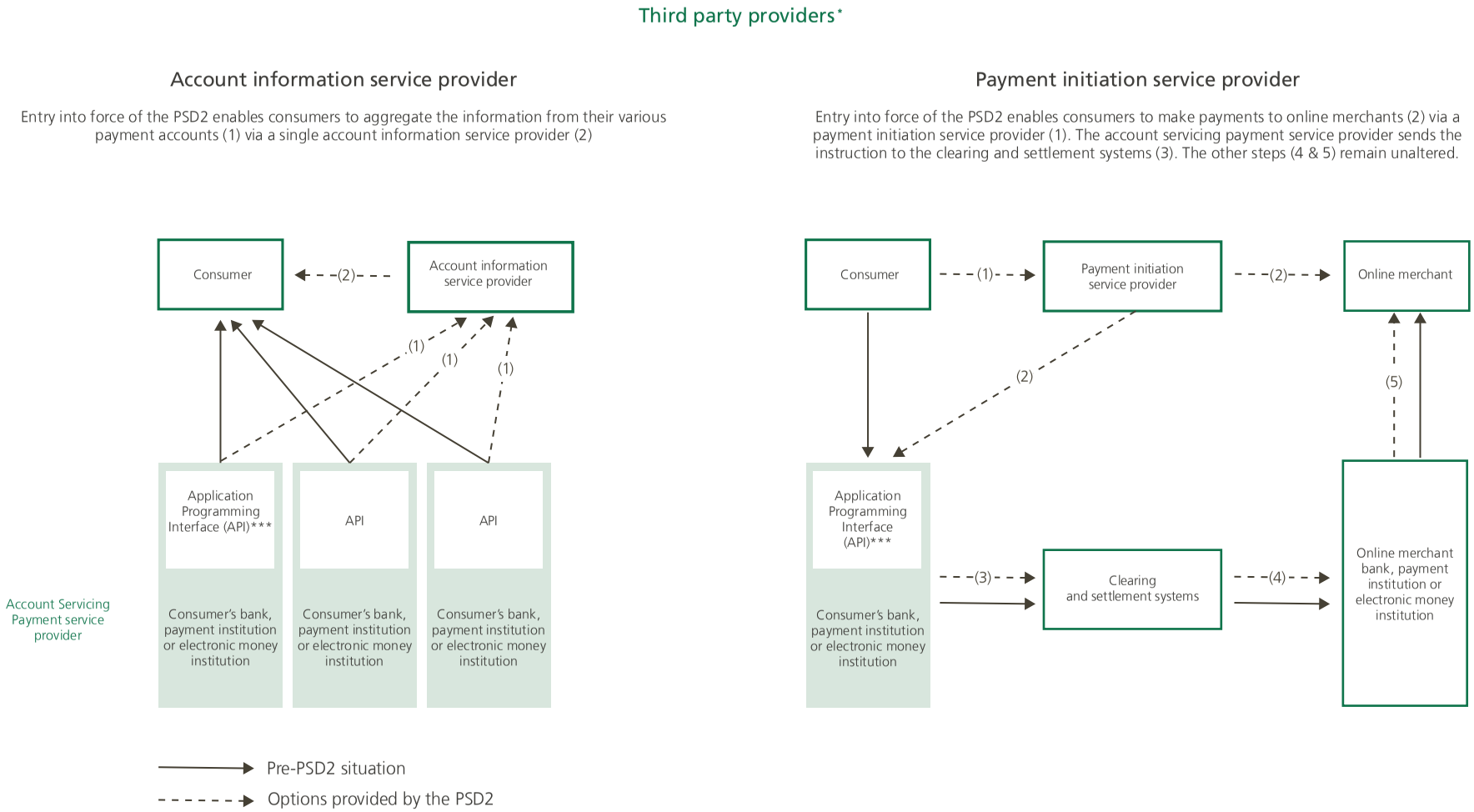
The strong development of the digitisation in the financial sector is driven in part by the transposition of the second European Payment Services Directive (PSD2)[2]. This Directive, which was transposed into Belgian law by the Law of 11 March 2018, is related to recent innovations in the payments sector and requires payment service providers to open up their payment account infrastructure (Open Banking). This should enable new players to enter the payment services market and offer payment initiation and account information services. The opening up of the payment accounts infrastructure is accompanied by strong security requirements with which payment service providers (banks, payment institutions and electronic money institutions) must comply.

1 InsurTech refers to the use of technological innovations to achieve savings and increase the efficiency of the current insurance sector model. InsurTech explores the opportunities, such as the supply of ultra-personalised policies and the use of new data flows from internet devices, for dynamic assessment of premiums according to observed behaviour.

2 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.

Chart 104

Diagram of the operational processes relating to the new payment services



Source : NBB.

(*) Third party provider: a third party may be (1) a payment initiation service provider, authorized by the Bank and subject to more limited regulatory requirements (given they do not come into possession of customers' funds), or an account information service provider, registered by the Bank (which also does not come into possession of customers' funds). Third party providers may also be banks, payment institutions or electronic money institutions.

(**) Account Servicing Payment service providers: banks, payment institutions or electronic money institutions authorised by the Bank and subject to its prudential supervision.

(***) API: Application Programming Interface.

To that end, the PSD2 introduces two new categories of payment service providers in the regulatory framework, payment initiation service providers and account information service providers. Like other institutions approved for that purpose, these two types of service provider will be able to access the payment accounts of a payment service user subject to the user's explicit consent. One of the possible applications of this change in the legal framework is the opportunity for an account information service provider to consolidate the account balance of multiple payment accounts held by an individual with multiplefinancial institutions, in one single application. For payment initiation service providers, the new regulatory framework enables them to initiate payments directly from the payment account of a user to the beneficiary. The diagram below illustrates the new business models that are made possible on the basis of the new legislative framework.

Existing credit institutions, payment institutions and electronic money institutions will also be able to offer these new services. Thanks to this new legislative framework, all these players will be able, at the request of their customers, to consult their payment accounts or initiate payments from accounts held by that customer with another financial institution. For payment service users, be they individuals or legal entities, it will thus become possible to manage all their payment accounts via a single application of just one service provider. This development should further intensify competition between financial service providers to retain their customers and acquire new ones.

Given that new types actors can obtain access to payment accounts, an important pillar of this new Open Banking landscape conssits of additional IT and security provisions that need be respected by the industry. More specifically, this concerns the application of strong customer authentication for the secure initiation and execution of payments, and the implementation of common, secure and open communication standards for the interaction between account servicing payment service providers (i.e. banks, payment institutions and electronic money institutions), account information service providers and payment initiation service providers. In order to ensure uniform application of these new regulations accross the EEA, the EBA is in charge of developing the technical standards on the subject.

Strong customer authentication requires the use of at least 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 inherent to the user (e.g. biometric data such as a fingerprint). Given that the regulatory technical standards are both technology and business-model neutral, market players are able to develop new products that take into account these requirements. For instance, there are already payment cards that use a fingerprint instead of a PIN code for the purpose of applying strong customer authentication.

In regard to communication requirements, the PSD2 introduces the obligation for account servicing payment service providers to offer at least one interface to account information service providers and payment initiation service providers for accessing information on the payment accounts that they manage. The existing practice of third-party access without identification, referred to in market jargon as 'screen scraping' or, mistakenly, as 'direct access', will no longer be allowed once the regulatory technical standards apply, as of 14 September 2019. It is important to note that these technical standards only apply to payment accounts, in accordance with the scope of the PSD2. The standards therefore do not apply to access to accounts which are not to be qualified as payment accounts.

Entry into force of the PSD2 Directive gives new actors access to the payment services market

The development within the payments market and the Open Banking landscape will demonstrate whether the various objectives of the PSD2, such as the promotion of competition and innovation, fostering the integration of payments within the EU, and enhancing customer convenience, will be achieved.

5. Cyber risks and IT risks

5.1 Continuing rise in cyber threats and IT-related threats

The digitisation of the operational processes of the financial sector, which is already highly computerised, progressed further during the year under review. The degree of interconnectivity between

the operational processes of the various financial players also remained very high. Moreover, financial institutions are increasingly opting for business models in which IT services are outsourced according to operational or functional specialisation. The increased and more diversified digitisation of access channels for customers of financial institutions and FMIs is another factor adding to the complexity of the financial landscape and the rise in operational risk.

Throughout the world, cyber attacks are becoming ever more sophisticated and powerful, and the financial sector is one of the potential targets (see box 17). The number of targeted, long-term cyber attacks is likely to grow further in the future. Cyber attacks may come from inside or outside the institution, and the attackers may have various motives, ranging from financial theft to geostrategic espionage and sabotage, and including terrorism and activism. Cyber criminals' ability to conceal the attack in certain cases permits misappropriation over long periods, intentional disclosure, and the modification or destruction of sensitive or critical financial data.

In these circumstances, it is hard for financial institutions and FMIs to provide adequate protection against the various attacks for their IT systems and services and their electronic data. As cyber threats are evolving very rapidly, it is more important than ever to ensure that the defence capabilities of institutions and FMIs enable them to respond flexibly to the changing attack methods. In this context, solutions for gathering information on the potential threats, attackers and types of attack are vital. In addition, it is useful for financial institutions to know the customer's and/or counterparty's risk profile in order to determine the risk of fraud associated with certain transactions. In retail banking, for example, that is achieved by means of security mechanisms integrated in the internet or mobile banking application. In the case of correspondent banking activities, one example is the Customer Security Programme (CSP), set up by SWIFT to facilitate assessment of the counterparty risk.

It is more important than ever to ensure that the defence capabilities of institutions and financial market infrastructures enable them to respond flexibly to the changing cyber threats

Apart from cyber risk, the financial sector's heavy dependence on IT solutions also presents other challenges. Under pressure from innovative players, new technologies, customer expectations or growing security risks, traditional institutions are encouraged to renew their sometimes very obsolescent IT architecture, but the complexity of their IT environment makes it very hard to achieve that aim quickly and responsibly, i.e. without taking disproportionate risks. There is likewise a high risk of growing dependence on third parties for IT services and standardised IT system components. In particular, cloud solutions are increasingly being used, and for ever more important processes. The need for sufficiently representative testing of recovery solutions – which must guarantee continuity following incidents – remains another key point for attention.

It is therefore essential for the management bodies of the financial players to have the necessary expertise and information to enable them to keep a proper watch on the risks and contain them within acceptable limits. In addition, all the staff of these businesses must be aware of cyber risks and IT risks in order to understand how those risks may arise and how they are expected to respond to them.

Assessing cyber risks and IT risks and promoting their control are similarly 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 IT risks and cybernetic risks. Due attention is also being paid to the intersectoral control strategies being devised in Belgium and abroad. These two aspects are discussed in more detail in the sections below.

BOX 17

Some examples of cyber security incidents and threats in 2018

Meltdown / Spectre: In January, vulnerabilities specific to the speculative execution technique were exposed, this technique consisting in processor optimisation which is invariably applied in (all) modern processors. Although chip manufacturers have meanwhile updated the microcode as far as possible, in order to limit the scope for exploiting these vulnerabilities, it is likely that ultimately only an adjustment to the hardware of the future processors will provide full protection. For now, the financial sector has not experienced any specific incident based on exploitation of these vulnerabilities.

Coincheck Inc: In January, it was reported that fraudsters had stolen over 500 million in XEM cryptocurrency, the currency specific to the NEM (New Economy Movement) blockchain platform. At the time of the incident, the stolen XEM cryptocurrencies represented around $ 400 million. A trading platform for these cryptocurrencies, Coincheck, was hacked.

Mexico: In May, it transpired that a number of Mexican banks had fallen victim to a cyber attack. The fraudsters had credited false accounts and then withdrawn large sums in cash. Customers' accounts were unaffected by the attack. According to the reports, the fraudsters succeeded in abusing software modules developed by the banks or third parties enabling transactions via a local Mexican interbank payment system. The local interbank payment system itself was not compromised; it was only the access points to this network in individual institutions that were affected.

Supermicro: In October, there were widespread media reports of the potential manipulation of Supermicro motherboards during the production process, which would make these hardware components vulnerable to espionage. Since these motherboards are used throughout the world in server infrastructures, the potential impact was massive. But, following an investigation, Supermicro stated that no evidence had been found to support the allegations previously publicised by the media. Nonetheless, these disclosures drew attention to the danger of cyber attacks via the suppliers of hardware, software and IT services. Earlier in 2018, the American and British authorities had explicitly warned against the danger of this type of attack.

5.2 Guidelines on cyber risk resilience

In recent years, the Bank has made a substantial contribution to the preparation of a regulatory framework aimed at improving the control of cyber risks and IT risks. On 1 January 2016, the prudential Circular[1] on the Bank's expectations concerning the operational continuity and security of systemically important institutions came into force. The Bank also made an active contribution to establishing a European regulatory framework for the management of IT risks and cyber risks under the aegis of the EBA. That work culminated in the publication by the EBA of guidance for supervisory authorities on the assessment of the ICT risk in the SREP (Supervisory Review and Evaluation Process) of credit institutions and investment firms[2], which

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.

came into force on 1 January 2018. It also led to EBA recommendations on outsourcing by financial institutions to cloud service providers . In addition, the EBA published various technical recommendations, guidelines and standards in connection with the second European Payment Services Directive (PSD2), covering cyber and IT aspects. Furthermore, the EBA is preparing guidelines on outsourcing in general and on management of ICT-related risks and security risks.

Various initiatives were also taken for FMIs in this respect. In June 2016, the Committee on Payments and Market Infrastructures (CPMI) and the International Organisation of Securities Commissions (IOSCO) published guidelines on cyber resilience[2], which are applicable immediately to FMIs. During the year under review, on the basis of these guidelines, the Eurosystem drew up the Cyber Resilience Oversight Expectations (CROE), which were finalised in December 2018 after a public consultation cycle. In May 2018, the CPMI published a strategy[2] for reducing the risk of wholesale payments fraud. This strategy proposes measures for preventing,

1 EBA recommendations on outsourcing to cloud service providers, December 2017.
2 CPMI-IOSCO, Guidance on cyber resilience for financial market infrastructures, June 2016.
3 Reducing the risk of wholesale payments fraud related to endpoint security (https://www.bis.org/cpmi/publ/d178.htm).

detecting and remedying fraud, and highlights the need for proper communication on the subject by all the public and private sector players concerned. As co-chair of the CPMI working group, the Bank made a significant contribution to that strategy. Like the other member central banks, the Bank is also working on the implementation of this strategy.

5.3 Operational activities

Cyber and IT risks are a major point of attention for the Bank in the course of its prudential supervision and oversight. In that sphere, it focuses attention 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 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 play a central role here. In 2018, 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 also devotes increasing attention to sector-wide initiatives. For instance, the SSM regularly conducts cross-sectoral analyses on subjects relating to IT and cybernetic aspects. In 2018, for example, it asked all the significant banks and the largest less significant banks to answer a questionnaire which should supply important information on IT aspects for the annual SREP, and will also permit cross-sectoral analyses.

In its role as the sectoral authority for application of the law on the security and protection of critical infrastructures (principally banks and FMIs), the Bank also assesses the effectiveness of the control systems of these infrastructures, organises sectoral exercises and coordinates operational incidents of a systemic nature for the Belgian financial sector.

In order to implement the recommendation of the High Level Expert Group (HLEG) on the future of the Belgian financial sector, namely to pay sufficient attention to cyber security, the Financial Sector Cyber Advisory Council (FSCC) was set up under the chairmanship of the Bank. It comprises representatives of the Centre for Cyber Security Belgium, Febelfin, Assuralia and the financial sector. The FSCC endeavours to boost the cyber resilience of the Belgian financial sector via a range of initiatives.

One practical achievement here is the establishment of an ethical hacking framework by the Bank, namely TIBER-BE (Threat Intelligence-Based Ethical Red Teaming Belgium). This programme forms the Belgian part of a methodology devised by the Eurosystem and aiming to increase the cyber resilience of individual financial institutions and FMIs by means of sophisticated tests, and to supply important observations on 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.

The Bank has set up an ethical hacking framework which aims to increase the cyber resilience of financial institutions and financial market infrastructures

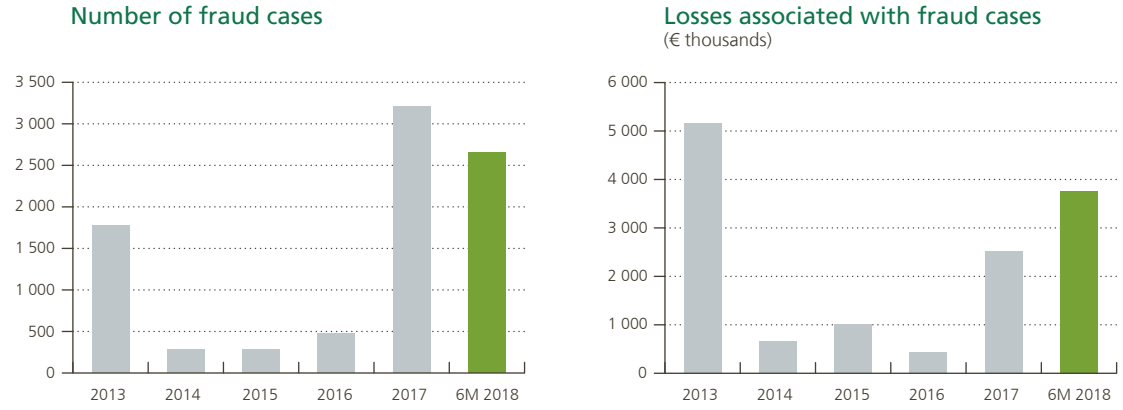
5.4 Internet banking fraud

The close cooperation with Febelfin and other parties continued in 2018 for the purpose of mapping e-banking fraud and raising consumers' awareness. The clear upward trend in the number of e-banking fraud cases apparent in 2017, and the associated financial losses, was confirmed in the first half of 2018.

As in previous years, reported cases of e-banking fraud among consumers in 2018 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 rise in fraud cases in 2017 and 2018 is therefore attributable to an increase in the number of attacks rather than the use of innovative fraud techniques.

Chart 105

E-banking fraud



Source : Febelfin.

Here, too, the Bank keeps a very close watch on the changing risks associated with the entry into force of the PSD2.

6. Developments in governance, reporting and auditors' cooperation in prudential supervision

Expertise of compliance officers

The 2016 report of the High Level Expert Group (HLEG) on the future of the Belgian financial sector contained a series of recommendations on strengthening governance in financial institutions. In 2017, it had already led to changes to the various sectoral laws, notably to enable the Bank to impose the same expertise requirements on compliance officers as those already applied by the FSMA. Consequently, in 2018, the Bank and the FSMA developed a common approach in order to harmonise more closely the requirements of the two supervisory authorities in regard to assessment of the expertise of compliance officers. These requirements were laid down in a Bank Regulation [1].

The main new point concerns candidate compliance officers having to pass an examination at a training centre accredited by the Bank and the FSMA. On 18 May 2018, the two authorities published a joint Communication [2] on this subject, setting out the procedure which institutions wishing to hold examinations must follow in submitting their application for accreditation to the two supervisory authorities. The application for accreditation must include the information permitting verification that the tests meet all the accreditation conditions (content of the questions, composition and working method of the board of examiners, practical organisation, etc.).

From now on, compliance officers and other persons responsible for the compliance function must also take part in an ongoing training programme in a training institution recognised by the FSMA on the Bank's recommendation. In that connection, on 8 May 2018 the FSMA published a Communication [3] specifying the scope of that ongoing training obligation, notably as regards the course frequency and content.

Renewal of auditors' accreditation

In view of the societal importance of financial institutions and insurance companies, auditing duties can

1 Bank Regulation of 6 February 2018 on the expertise of persons responsible for the compliance function, approved by Royal Decree of 15 April 2018 and entered into force on 1 June 2018.

2 Communication NBB_2018_19 of 18 May 2018 on applications for accreditation of examinations with a view to performance of the compliance function.

3 FSMA_2018_05 Communication of 8 May 2018 on ongoing training for officers.

only be entrusted to auditors approved for that purpose by the Bank. The Bank grants auditors accreditation for a six-year period on the basis of the Bank's accreditation Regulation of 21 December 2012[1]. No earlier than six months and no later than three months before that accreditation expires, the accredited auditor must on his own initiative apply for renewal of the accreditation for a further six-year period. The first renewal applications should arrive at the Bank during the first quarter of 2019.

In this connection, on 21 September 2018, the Bank published a Communication[2] explaining the form and content of the application for renewal of the accreditation. That Communication lists the information which the application must contain, including as regards the experience gained in the course of mandates for institutions subject to supervision (description of the mandates, assessment of the cooperation with the Bank, plan of approach for the future). The aim is to obtain specific information supplementing the accreditation application, to enable the Bank to check whether the information tallies with the records which it has created over the years in the course of a system of annual assessment of the quality of the auditor's work per mandate exercised in a supervised institution. In accordance with the accreditation regulation, the Bank has to justify any decision to refuse renewal of accreditation in regard to the expectations concerning the competence requirements and the efforts made in carrying out the assignment.

1 Bank Regulation of 21 December 2012 on the accreditation of auditors and firms of auditors.

2 Communication NBB_2018_26 of 21 September 2018 on the renewal of auditors' accreditation.

Follow-up to parliamentary recommendations

After publication of the recommendations of the parliamentary commissions concerning Optima[1] and Panama Papers[2], the Bank cooperated fully in various regulatory initiatives, notably in regard to transactions between related parties and special mechanisms.

Modification of the legal framework governing transactions between related parties was also recommended by the IMF in the 2017 FSAP (see chapter A of the "Prudential regulation and supervision" part), in order to comply with the Basel Committee's fundamental principles for effective banking supervision (principle 20 - transactions with related parties). The sectoral laws already specify that loans, credits or guarantees must be concluded on the conditions applicable to their customers and must be notified to the statutory management body and to the supervisory authority[3]. In order to implement the recommendations, an amendment to these rules was prepared, which extends both the material scope (all transactions between related parties) and personal scope (all intra-group transactions, including transactions with subsidiaries and sister companies).

In order to implement the recommendations of the two parliamentary commissions on tax evasion (special mechanisms), a working group was set up comprising representatives of the Ministry of Finance, the Treasury, the Special Tax Inspectorate, the FSMA and the Bank.

This working group tackled three subjects:

- adjustment of the legal framework concerning special mechanisms, in order to make it easier to report them to the justice system;
- updating of the list of special mechanisms, with examination of mechanisms which may be deleted from existing Circulars[4], those which may be reformulated, and those which should be added; and
- conclusion of a cooperation agreement with the Special Tax Inspectorate so that information useful for the supervision of a financial institution can be passed on to the Bank and the FSMA.

Suitability of directors and other key function holders

The prudential legislation stipulates that directors, members of the management board, those responsible for independent control functions and those effectively managing financial institutions must have the expertise and professional integrity required for their job. The assessment of the suitability of these persons is often described as the assessment of their "fit & proper" character.

In the wake of the financial crisis, the question of "suitability" has been a priority for some years and has given rise to the publication of a series of new rules, guidelines and recommendations at international, European and national level.

For instance, on 26 September 2017 the EBA and ESMA published joint guidelines on the assessment of the suitability of members of the management body and key function holders[5]. The ECB also recently published its SSM Guide to fit and proper assessments[6]. In the insurance sector, the EIOPA Guidelines on the system of governance[7] provide a reference framework for the assessment of both the individual and collective suitability of directors and those responsible for independent control functions in insurance undertakings.

In view of the proliferation of rules and guidelines on the subject, some updating and some form of codification were necessary in order to maintain

1 On 7 July 2016, a parliamentary commission of inquiry was set up, and on 28 June 2017 it published a report on the failure of Optima Bank: in this connection, see "Parliamentary inquiry into the causes of the failure of Optima Bank and the possible conflict of interests between the Optima Group and its components on the one hand, and the government on the other", Parliamentary papers, 2016-2017, Doc. 54 1938/007.

2 On 21 April 2016, a special commission on "International tax evasion/*Panama Papers*" was set up which published its report on 31 October 2017: see: "The *Panama Papers* and international tax evasion", Parliamentary papers, 2016-2017, Doc. 54 2749/001.

3 See Article 72 of the Banking Law and Article 93 of the Solvency II Law.

4 This concerns more particularly two Circulars dated 18 December 1997, namely Circular D1 97/9 to credit institutions and Circular 97/4 to investment firms, and Communication D 207 of 30 November 2001 to insurance undertakings.

5 EBA/GL/2017/12 Guidelines of 26 September 2017 on the assessment of the suitability of members of the management body and key function holders. With effect from 30 June 2018, these guidelines replace the EBA GL 2012/06 guidelines of 22 November 2012.

6 SSM Guide to fit and proper assessments, May 2018.

7 EIOPA Guidelines on system of governance of 14 September 2015, in particular guidelines 11 to 14.

a good overview of the framework applicable. On 18 September 2018 the Bank therefore published a new "fit & proper" circular[1], aimed at creating a "fit & proper" manual and transposing the aforesaid EBA and EIOPA guidelines into the Belgian prudential framework.

The aim of the "fit & proper" manual is to list all the regulatory and policy documents applicable on the subject and provide the necessary clarification. In addition, the manual contains explanations on topics not covered in themselves by specific policy documents. The manual combines an intersectoral approach with the text and references specific to the various sectors: where the manual and its basic principles are applicable to all financial institutions subject to the Bank's supervision, the relevant legal and policy texts applicable to the various types of financial institution are specified.

In terms of content, the manual is based on the guidelines listed in the 2013 "fit & proper" Circular, which was repealed when the manual was introduced. In addition, the manual develops or highlights a range of subjects. For instance, further emphasis was placed on the primary responsibility of the institutions in the assessment of suitability, and there was development of the chapters on collective suitability, continuous suitability assessment (and therefore, if necessary, reassessment of the person concerned), and the time which must be devoted to performing the duties of a director. The manual also sheds light on a range of new points concerning expertise, such as the Bank's regulation on the persons responsible for the compliance function[2] (see above). As regards propriety, the manual now explicitly states that the lack of transparency in relation to the supervisory authority and breaches of the anti-money laundering legislation, consumer protection legislation and tax legislation, are points to be taken into account in assessing the suitability of the person concerned.

Specifically for the banking sector, the manual deals with some particular points concerning the EBA guidelines and the SSM supervision. Thus, in the manual the requirements on the number of years of relevant professional experience for directors of significant institutions subject to ECB supervision are aligned with the thresholds defined in the SSM Guide. Decisions on suitability which are the responsibility of the ECB are subject to slightly longer timescales, in line with current practice. Finally, the chapter on directors' independence and the management of conflicts of interest clarifies the way in which the provisions on these subjects under the Banking Law are to be read in connection to the guidance on these topics in the EBA guidelines.

In the insurance and reinsurance sector, the 2013 rules on expertise and integrity were generally kept on in the new manual. Nonetheless, a number of points were added, notably in connection with the Solvency II rules: (i) obligation to develop a "fit & proper" policy, (ii) explicit mention of the basic theoretical knowledge expected in the field of insurance and reinsurance, (iii) listing of specific rules on the expected expertise of persons responsible for independent control functions, (iv) definition of expertise rules to be respected for "reference persons" to be appointed within the undertaking if an independent controlfunction is outsourced, and (v) the recommendation whereby, in the case of financial conglomerates in which there are significant business relationships between the bank and the insurer, the insurer's board of directors should include one independent director within the meaning of Article 526*ter* of the Company Code who does not have a seat on the board of directors of the bank and the parent company. In addition, the rules followed by the Bank in its suitability assessment were also reviewed ("fit & proper" interview, modelling of the Bank's decisions, etc.).

The question of suitability (fit & proper character) has been a national and international priority for some years

Since this manual is, in principle, an evolving document which is published on line, it will be modified regularly in accordance with new developments on the subject so that, in the future, institutions will continue to have an updated overview of the prudential framework in this area.

1 Circular NBB_2018_25 of 18 September 2018 on the suitability of directors, members of the management committee, responsible persons of independent control functions and senior managers of financial institutions.

2 Royal Decree of 15 April 2018 approving the National Bank of Belgium Regulation of 6 February 2018 on the expertise of persons responsible for the compliance function.

7. Brexit

On 29 March 2017, following the referendum on departure from the EU, the United Kingdom had initiated a procedure provided for in Article 50 of the EU Treaty with a view to leaving the EU and thus becoming a "third country". Unless a different date is specifically agreed, the whole legal framework of the EU will cease to apply to the United Kingdom from 30 March 2019. In particular, financial institutions might lose their European passport which previously conferred freedom to provide their services in every EU country.

Since May 2017, the EU and the United Kingdom have been negotiating their separation agreement in order to avoid the serious consequences of a disorderly ("hard") Brexit. Such a scenario means great legal uncertainty for current business relationships, and risks causing a sudden interruption in services which will have a serious impact on economic activity. Both parties are committed to reaching agreement, but material differences between the two camps could prevent an agreement from being concluded. If the agreement is ratified, it could include a transitional period up to 31 December 2020.

In view of the said uncertainty, the European Commission has reminded all parties concerned of the importance of preparing for a "hard Brexit" which could materialise as early as March 2019. In that context, the European supervisory authorities and the ECB have issued opinions and clarified their expectations for the financial sector. The Bank has repeatedly drawn the attention of Belgian financial institutions to the risks that would result from a "hard Brexit" by referring to the opinions published by the EBA, surveys of the sector and prudential measures in relation to the institutions concerned.

The Bank has made financial institutions aware of the risks that would result from a hard Brexit

In order to guarantee the continuity of their activities, financial institutions may need to apply to the national competent authorities for a new licence, amend certain clauses in their contracts or transfer certain activities.

The Bank notes that, overall, the level of exposure of the Belgian financial sector to British counterparties is relatively low. At the end of June 2018, those exposures totalled € 39 billion for Belgian banks, or 4 % of their total assets, and € 6 billion for Belgian insurers, corresponding to 2 % of their investments.

However, the potential impact of a hard Brexit is not confined to direct exposures, and depends both on the nature of the undertaking's activities and the level of preparation required, which varies from one institution to another.

Although they do not provide services for customers directly in Britain, many institutions could be affected via contracts concluded with British counterparties. For example, there is legal uncertainty over the possibility of making changes or exercising certain options under existing over-the-counter derivative contracts which are not handled by a clearing house (central counterparty, CCP). To reduce that risk, institutions should check the cases in which authorisation has to be obtained from the competent national authorities (the FSMA in Belgium and the Financial Conduct Authority in the United Kingdom). Moreover, bonds issued by Belgian banking institutions but governed by British law might not be eligible for a bail-in, so that certain changes would need to be made to the issuance contract clauses.

British CCPs perform a critical role for the European financial market, as they clear more than 90 % of the transactions in interest rate derivatives in Europe. At present, British CCPs are subject to the European Regulation on over-the-counter derivatives (European Market Infrastructure Regulation, EMIR). They risk losing their licence to effect clearing of these products in Europe. The massive and sudden interruption of the clearing services of British CCPs could cause serious instability on the financial markets. In order to reduce the dependence of European financial institutions on British CCPs, the European authorities are encouraging them to establish access to CCPs based in the European Union, outside the United Kingdom. However, to avoid serious disruption to current activities, the Commission will grant a temporary licence extension to British CCPs. With a view to improving the regulation of the activities of systemically important CCPs based in third countries, including – after Brexit – the United Kingdom, the European Commission envisages modifying the EMIR Regulation to give greater power of supervision of those entities to the European Financial Markets Authority.

A number of Belgian banks provide banking services in the United Kingdom. The Bank has asked them to contact the British authorities in order to ensure the continuity of those activities. They must also inform their customers in time, notably if the services are modified or terminated.

Similarly, in order to ensure the continuity of their commitments to British customers, some Belgian insurers need to establish a British branch or subsidiary. Establishment of such an entity is subject to the approval of the British authorities and the Bank's non-objection.

In the wake of Brexit, British insurers are liable to lose their right to offer protection to customers in the European Economic Area (EEA). In that context, some British insurance companies have already begun setting up subsidiaries in Belgium. Having an establishment in Belgium will also enable them to pursue their activities in other countries of the European Economic Area, either under freedom to provide services, or via branches. In addition, insurers must ascertain that they can still settle claims under existing insurance contracts held by EU customers. Many of them have already taken steps to transfer their contracts to an EU-based entity. That takes time, because it requires not only the approval of the national prudential supervision authorities in the EU and the United Kingdom, but also the approval of the British Court of Justice.

The same applies to British payment institutions, electronic money institutions and investment firms, which will lose their passport, essential for continuing to do business with their customers in the EU. To guarantee the continuity of their services in Belgium and the EU, a number of institutions have

applied to the Bank for approval or are considering doing so.

The Bank's prudential supervision teams have conducted numerous dialogues with Belgian financial institutions, which have evidently made good progress in identifying the risks and preparing for the potential consequences of a hard Brexit. The Bank is likewise in discussions with institutions which are considering modifying their structure or wish to establish a branch or subsidiary in Belgium to offer services to EU customers.