

E. Financial market infrastructures

1. Introduction

There were further developments in the legislation on financial market infrastructures (FMIs) during the year under review. Section 2 presents the mapping of the sector. The oversight approach is traditionally based on principles rather than on detailed rules; the authorities use arguments to persuade FMIs (moral suasion) instead of punishing them with fines or other penalties. However, there is an evident shift away from this soft law approach towards hard law in the sense that the requirements are spelt out in laws for both payment systems and CSDs. Where CSDs are concerned, the Regulation on central securities depositories (the CSD Regulation)⁽¹⁾ transposes

into European law the CPMI-IOSCO Principles for Financial Market Infrastructures. Apart from the publication of the Circular on recovery plans for FMIs, the main provisions of which are discussed in section 4 of the chapter on “Recovery and resolution”, the regulations were further extended as explained in section 3 of this chapter.

Section 4 describes the supervision and oversight activities relating to the risks accorded priority attention in the Annual Risk Review 2015. More specifically, this concerns supervision of liquidity and credit risk, operational risk and the monitoring of the business models.

(1) Regulation (EU) No. 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No. 236/2012.

2. Mapping of the sector

The Bank is responsible for the oversight and prudential supervision of FMIs. The prudential supervision monitors the risks facing the FMI itself, while the oversight focuses on the security and efficiency of the system operated by the FMI. In particular, the oversight checks whether systemic infrastructures are capable of ensuring the continuity of their services in extreme circumstances. The table shows the Belgian infrastructures subject to the Bank's authority and the cooperation

between the Bank and the supervisory authorities of third-country infrastructures.

The Bank grants authorisation for payment and electronic money institutions. The number of payment institutions has risen slightly since last year: one institution was licensed with full status (B+S Payment Europe) and two exempt institutions were authorised to offer payment services in Belgium (Rent A Terminal Belgium SPRL and

TABLE 7 THE BANK'S SUPERVISION AND OVERSIGHT OF FINANCIAL MARKET INFRASTRUCTURES

	Institutions / systems subject to supervision and oversight		
	The Bank acts as the sole authority	International cooperation	
		The Bank acts as the lead authority	The Bank participates, another authority is lead authority
Prudential supervision	Belgian branch of Bank of New York Mellon (BNYM)		BNYM SA/NV
	Payment and electronic money institutions		
Supervision and oversight	BNYM CSD Worldline Belgium	Euroclear Bank Euroclear Belgium Euroclear SA/NV	CCP Colleges ⁽²⁾
Oversight	NBB-SSS Bancontact / MisterCash ⁽¹⁾ Centre for Exchange and Clearing ⁽¹⁾ MasterCard Europe ⁽¹⁾	SWIFT ⁽³⁾	TARGET2 TARGET2-Securities CLS ⁽⁴⁾

Source : NBB.

(1) Peer review in the Eurosystem / ESCB.

(2) These are the supervisory colleges for the central counterparties LCH.Clearnet SA, LCH.Clearnet Ltd, EuroCCP, Eurex AG Clearing, CC&G, ICE Clear Europe, KDPW-CCP and Keler CCP.

(3) Society for Worldwide Interbank Financial Telecommunication.

(4) Continuous Linked Settlement.

Belmoney Transfert SPRL). One exempt institution ceased its activities. Two of the three new institutions operate in card payment systems, which reflects the changing market conditions in the card payment sector. In the electronic money sector, there were no changes in the number and status of the institutions in 2015. Altogether, there are 20 institutions offering payment services in Belgium and 11 which can issue electronic money; this number is set to rise owing to the new regulatory framework applicable to payment services.

TABLE 8 NUMBER OF PAYMENT AND ELECTRONIC MONEY INSTITUTIONS SUBJECT TO SUPERVISION

	31-12-2014	31-12-2015
Payment institutions	18	20
Under Belgian law	11	12
Exempt institutions ⁽¹⁾	4	5
Branches governed by the law of an EEA member country	3	3
Electronic money institutions	11	11
Under Belgian law	5	5
Exempt institutions ⁽¹⁾	5	5
Branches governed by the law of an EEA member country	1	1

Source: NBB.

(1) Pursuant to Article 48 of the Law of 21 December 2009, "exempt institutions" are subject to a lighter regime comprising only the obligations arising from Articles 21 and 22 of that Law.

3. Legislation

In the wake of the operational incidents at Worldline SA in 2014 and 2015, it was suggested that it might be advisable to introduce a stringent law governing the supervision of payment systems in Belgium. Worldline handles virtually all Bancontact/Mister Cash transactions in Belgium and a large proportion of other card payments. Consequently, Worldline is systemically important for payment transactions on the Belgian market and the company is subject to the oversight of the Bank.

After many years without a hitch, there have been seven incidents altogether in the past two years, three of which attracted extensive media coverage, while the others had little or no impact on the general public's payment transactions. Since operational continuity is crucial to the smooth flow and reliability of payments traffic in Belgium, questions were asked about whether oversight based on soft law is sufficiently effective. The current oversight role, based on moral suasion, may therefore be supplemented by hard law in order to safeguard the efficiency and stability of critical payment infrastructures.

A more stringent supervision law might, for example, impose requirements on payment transaction and payment scheme operators in Belgium in regard to such matters as operational stability (data confidentiality and integrity and system availability), transparency and communication. The stability and continuity of the processing of payments in Belgium must continue to be guaranteed, not least because the payment card industry is slowly but surely progressing towards a Single Euro Payments Area (SEPA), with moves to consolidate in order to achieve economies of scale, which could have a significant impact on the national payment infrastructures.

As foreseen by the 2007 Payment Services Directive, the EC launched a review in 2012 which led to a revision of the Directive in 2015. To make payment

services more transparent and competitive, the European Parliament and the Council broadened the playing field under the new Directive⁽¹⁾, paying particular attention to the security of payment services offered to the public. The revised Payment Services Directive, published on 23 December 2015, has to be transposed into national law by 13 January 2018. In comparison with the previous Directive, the scope has been extended to two types of payment services which were not previously subject to authorisation: payment initiation services and account information services.

Payment initiation services and account information services never hold the payers' funds. They only provide services to initiate payments or to collect account information with the express approval of the payment services user. They must ensure that personal security data are not accessible to other parties, and must communicate with the parties concerned in a secure manner. To ensure that any incidents are followed up directly and speedily, payment service providers will be obliged to report any significant operational or security incidents.

The new Directive also makes provision for the creation of a central register at European level containing lists of all payment institutions authorised in Europe. This will enable all payment service users to consult a central register comprising the data from all national registers of payment service providers.

Although cryptocurrencies (also known as virtual or digital currencies) such as Bitcoin do not constitute a payment system and the Bank has no authority over them, it keeps a close watch on the associated problems. As a payment

(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.

instruments regulator, it repeated the warning it issued in 2014 about the risks associated with virtual money. The Bank stressed once again that cryptocurrencies are not legal tender nor are they a form of electronic money, there is no financial supervision or oversight of cryptocurrencies, and these products are therefore risky. During the year under review, the Bank took part in two pieces of work on this subject. One was the ECB's February 2015 report entitled "Virtual currency schemes – a further analysis", which was an extension of an initial analysis of virtual currencies conducted in 2012⁽¹⁾, and the other was the report on digital currencies published by the CPMI⁽²⁾. Apart from the actual virtual currency schemes, the Bank is also interested in the new technologies that cryptocurrencies have brought (distributed ledgers) which could have a significant impact in the future on the operation of payment systems and instruments.

In regard to the CSD Regulation, last year saw the designation of the competent authority in Belgium, and further work on the technical standards. On 11 June 2015⁽³⁾, the Bank was designated as the competent authority responsible for carrying out the duties referred to in the CSD Regulation on the authorisation and supervision of CSDs, without prejudice to the specific responsibilities of the FSMA.

Three CSDs are currently operating in Belgium: Euroclear Bank, Euroclear Belgium and NBB-SSS. However, the authorisation obligation does not apply to this last CSD which is run by the central bank, although NBB-SSS has to conform to most of the requirements of the CSD Regulation. Furthermore, CSDs which themselves offer services relating to settlement in commercial bank money must obtain authorisation for the provision of banking-type ancillary services, in addition to their CSD and credit institution licences. That obligation applies to Euroclear Bank.

The CSD Regulation requires the Bank to consult the relevant authorities before granting authorisation to CSDs

or authorising the provision of banking-type ancillary services, and in reviewing the authorisations at least once a year. The authorities concerned, specified in the CSD Regulation, are the ones for which the smooth operation of the CSD is important, e.g. the overseer⁽⁴⁾ of the CSD, the central banks which issue the main currencies in which settlement is made, and the authorities of the countries for which the CSD is important. In that connection, it is worth noting that – separately from the CSD Regulation – the Bank intends to conclude an oversight cooperation agreement for Euroclear Bank, in accordance with the CPMI-IOSCO principles, with the central banks which represent the main currencies in the system.

The CSD Regulation empowers the European Securities and Markets Authority (ESMA) and the EBA to develop technical standards, in close cooperation with the members of the ESCB, and submit them to the EC, for the purpose of specifying the following in more detail (indicative list):

- the information that the CSD must supply to the competent authority in the authorisation application;
- the conditions under which the EU currencies are considered the main currencies;
- the reconciliation measures to be taken by the CSDs;
- the operational risks for links between CSDs and the methods of measuring, managing and reducing those risks;
- the financial instruments which can be considered highly liquid with a minimal market and credit risk, and in which the CSD is permitted to invest its financial resources;
- the tools for monitoring, measuring and managing (primarily intra-day) credit risks and liquidity risks.

The Bank was closely involved in the development of these technical standards which are scheduled for publication early in 2016. The CSDs must apply for the necessary authorisations on the basis of the CSD Regulation within a maximum of six months following publication of these technical standards.

(1) *Virtual currency schemes*, ECB, October 2012.

(2) *Digital Currencies*, CPMI, November 2015.

(3) Royal Decree of 11 June 2015 designating the competent authority responsible for the authorisation and supervision of central securities depositories.

(4) The Bank's responsibility as overseer is thus maintained as regards implementation of the CSD Regulation. In particular, that makes it possible to take account of changes in the international principles applicable to CSDs and impose compliance with those principles.

4. Oversight and supervision of FMIs

4.1 Liquidity risk and credit risk

During the year under review, the Bank played an active role in the discussions on the CSD Regulation's technical standards relating to liquidity risk. Moreover, that is one of the priorities of the 2015 Annual Risk Review for FMIs. In the case of international CSDs (ICSDs), liquidity risk is not only monitored as part of the prudential supervision but is also kept under close vigilance via oversight reporting which takes more account of the specific characteristics of FMIs. For instance, oversight reporting considers the intra-day risk (whereas prudential reporting is based on end-of-day figures) and reveals links with the settlement and other activities of the (I)CSD.

In view of the specific characteristics of (I)CSDs, and to supplement existing bank legislation, the CSD Regulation introduces rules on the management of intra-day credit risks and liquidity risks. In that connection, very close attention is paid to the management of the collateral that participants pledge to the (I)CSD. Another important point is the requirement for (I)CSDs to have sufficient liquid resources to cope with the simultaneous default of the two participants with the largest debit position. The CSD Regulation goes further here than the Principles for FMIs, which state that (I)CSDs must at the very least be able to withstand the default of the participant with the largest debit position.

Such stringent requirements are justified for CSDs in view of their systemic importance, as CSDs play a leading role in the settlement of stock market and off-exchange transactions between market counterparties. These systems are also used for mobilising and managing the collateral which is exchanged to cover the risks inherent in certain transactions, such as repos, or monetary policy or credit transactions, but also to meet the margin requirements of central counterparties (CCPs).

When CSDs process the purchase or sale of securities, the cash leg of the transaction is recorded on the account of either a central bank (central bank money) or a credit institution (commercial bank money). In the latter case, the CSD Regulation stipulates the use of a single-purpose bank, i.e. a credit institution which does not engage in any activities other than the settlement of the cash leg of securities transactions, in order to minimise the risks to that bank. In Belgium, the securities settlement systems settle transactions either in the books of the Bank (NBB-SSS and Euroclear Belgium) or in those of Euroclear Bank (the only future single-purpose bank in Belgium).

(I)CSDs that provide credit to their participants (in various currencies) – such as Euroclear Bank – may be exposed to credit risk and liquidity risk. This mainly concerns intra-day risks because, in principle, participants settle their accounts before the end of the day. Both the Principles for FMIs and the CSD Regulation require these credit risks relating to participants to be covered by collateral (or other equivalent financial resources). The Bank keeps a very close eye on the degree to which intra-day risks are covered at Euroclear Bank.

If a participant is unable to meet its liabilities, Euroclear Bank can liquidate the collateral. Since the proceeds of the liquidation or sale of the collateral are not available immediately, Euroclear Bank must have sufficient financial resources to bridge the gap. Part of the available liquid resources comes from the cash surpluses that participants leave on their account at Euroclear Bank. These can be used for routine liquidity risk management or – at least partially – in a crisis situation. While the surpluses contribute towards the liquid resources, they also create credit risks in that they are invested on the interbank market. The Bank pays due attention to the size of these cash surpluses and examines the degree to which the investments are covered by collateral (reverse repo).

Since Euroclear Bank's liquidity needs originate from providing credit to its participants, the Bank as the overseer keeps an eye on the trend in use of credit. In that connection, it takes a closer look at the links between the activities of Euroclear Bank and the resulting credit risks. Similarly, specific attention focuses on the liquidity needs and resources in various currencies, and the interdependence between Euroclear Bank and other market infrastructures such as CCPs or other (I)CSDs.

4.2 Operational risk

A second priority in the year under review was the operational risk including cyber risk (discussed in section 3 of the next chapter on "Cross-sectoral aspects of prudential regulation and supervision"). The oversight approach to operational risk goes well beyond the capital requirements for operational risk. Given the systemic importance of the financial market infrastructures, the availability of their systems is crucial. This aspect therefore takes up most of the attention in the monitoring of IT projects. Concerns about the timely delivery of a new platform or control of the associated costs must not take precedence over the stability of the financial system.

The Bank is the lead overseer of SWIFT (Society for Worldwide Interbank Financial Telecommunication). SWIFT is subject to central bank oversight because it is crucial to the security and efficiency of the financial messages exchanged between financial institutions and financial market infrastructures throughout the world. The oversight of SWIFT is conducted by the G10 central banks, while the oversight programme and findings are examined by a larger group in the SWIFT Oversight Forum, in which ten other central banks also participate.

The oversight activities concern all types of operational risks associated with SWIFT messaging services. Cyber risk was again the focus of greatly increased attention during the year under review. The development of mechanisms protecting against cyber threats is ongoing. As part of a continuous assessment, better ways of detecting, protecting against and responding to cyber threats are being examined, taking account of the changes in the nature of cyber threats and the new protection solutions gradually becoming available.

The modernisation of the FIN application, central to the SWIFT messaging services, continued during the year under review. This thorough technological overhaul was conducted without impairing the availability of the messaging services for customers. The monitoring of this multi-annual project was another key priority during the

year under review. In the past few years, there has been increasing diversification in the services that SWIFT provides for financial institutions, e.g. with the development of solutions assisting them in their reporting obligations to the supervisory authorities. Another point of interest for overseers is therefore the degree to which this increasing diversification of services influences the risk management of SWIFT as a whole.

4.3 Business model analysis

The monitoring of FMI's business models in a changing environment remains a priority for supervision and oversight. The growing need for collateral, and hence for collateral management services, is a trend that has been in evidence for some years now. The obligation to use a central counterparty for clearing standardised over-the-counter (OTC) derivatives will not only increase the need for collateral or margin, but will also mean that the frequency with which counterparties have to exchange collateral will increase from a weekly or monthly cycle for transactions not cleared in a CCP to more intra-day margin calls. In addition, many counterparties (including CCPs and central banks) have their own definition of eligible collateral. Market players who are very active on the repo markets or in multiple CCPs therefore need an efficient platform for transferring securities (sometimes even intraday) accepted by their various counterparties. In view of the market players' ever-increasing need for collateral, efficient allocation of the collateral is necessary to avoid any (real or apparent) shortages.

For quite a few years now, Euroclear Bank has offered collateral management services which were recently grouped under the name Collateral Highway. This platform enables customers to mobilise their securities efficiently (whether they are on an account with Euroclear or with a partner) and transfer them to the counterparty who needs them as collateral. These services are offered not only to customers of Euroclear Bank but also to customers of other CSDs in the Euroclear group, as the services have been extended to local Euroclear CSDs. The joint venture between Euroclear and the American CSD Depository Trust & Clearing Corporation (known as DTCC-Euroclear Global Collateral Ltd) is another major extension of the Collateral Highway. The joint venture will enable customers to manage their margin obligations efficiently and simplify the mobilisation of the necessary collateral (from the American CSD). Mid-2016 will see the launch of the first part of the platform, namely the Margin Transit Utility (MTU), which will handle the processing of margin obligations. The second part, the Collateral Management Utility (CMU), which will deal with the mobilisation of

collateral, will be launched a few months later. The Bank's approval was required in the same way as for all strategic decisions by systemic institutions. The competent authorities of the United States and the United Kingdom (as the joint venture is based in Britain) will also have to approve the project.

The business models of the Belgian BNYM entities were also monitored. This year, as part of an exercise whereby the group's presence, and its activities and the markets to which access is proposed, are continuously adapted to the financial and regulatory context, the BNYM group made various changes affecting the group entities in Belgium.

One important change with regard to its positioning is the group's decision to connect to the TARGET2-Securities platform as a directly connected participant. That decision implied direct access to TARGET2 for BNYM SA/NV and led to the gradual replacement of its access to the infrastructures of the main European markets via sub-depositors by direct access. The group consequently decided to put its central securities depository BNYM CSD SA/NV on standby.

The BNYM group also opted to refocus the activities of BNYM SA/NV on securities management, by terminating its activities as a member of clearing institutions on

behalf of its customers operating in derivatives and by transferring its securities lending and borrowing activities to the Bank of New York, London Branch.

The Crisis Management Group (CMG), set up in accordance with the FSB's guidelines on Key Attributes of Effective Resolution Regimes for Financial Institutions, is interested in the organisation of the BNYM group's activities, as this group is considered to be a Global Systemically Important Financial Institution (G-SIFI), i.e. an institution which, owing to its size, activities and deep embedding in the financial network, is of systemic relevance in the financial world.

Since 2013, a CMG meeting has been held every year for BNYM, organised alternately by the Federal Deposit Insurance Corporation and the Federal Reserve Bank of New York. The Bank is also represented on the CMG, as are the Board of Governors of the Federal Reserve System (United States), the Bank of England (United Kingdom), the Prudential Regulation Authority (United Kingdom) and – for the first time in 2015, as observers – the ECB and the Single Resolution Board (SRB). The CMG focuses in particular on the international configuration of the BNYM group, its presence in over 100 markets, the monitoring of transnational outsourcing and the degree to which its operational continuity can be guaranteed or improved.