

F. Financial market infrastructures

During the year under review, in regard to financial market infrastructures (FMIs), particular attention focused on changes in the regulations and their implementation by the systems and institutions subject to the Bank's prudential supervision and oversight activities. The possible implications of Brexit for this sector were also considered in detail. As in the case of other financial sectors, developments concerning FinTech (see section G.3. below) and cyber risks (see section G.4) were likewise closely monitored.

The Bank also published for the first time the Report on Financial Market Infrastructures and Payment Services⁽¹⁾, offering a detailed picture of the activities of those systems and institutions, changes in the regulatory environment, the Bank's approaches to oversight and prudential supervision, and its main objectives for 2017.

1. Mapping of the sector

Belgium hosts a number of FMIs, securities depositories, payment service providers such as payment institutions and electronic money institutions, and critical service providers. Some of these entities, such as SWIFT, Euroclear, Bank of New York Mellon, Mastercard Europe and Worldline, are of international systemic importance. As the lead authority, the Bank set up international cooperation agreements for some of these systems and institutions.

The Bank's oversight is concentrated both on the security and efficiency of all FMI operations such as payment, clearing and settlement systems, and on their connections with other financial market players. At microeconomic level, the prudential supervision authorities watch over the financial health of institutions in this sector, thus helping to maintain confidence among their counterparties and users. These two supervision approaches are aimed at promoting financial stability. In cases where the Bank exercises both oversight and prudential supervision, the supervisory activities can be considered complementary.

The systems and institutions can be grouped according to the type of services that they offer their participants or

customers: clearing, settlement and custody of securities, payments and the provision of critical services.

2. Priorities for oversight and supervision

In 2017, the Bank devoted a major part of its prudential supervision and oversight activities to changes in the legislation affecting most categories of FMIs and payment service providers, and to analysis of the impact of those changes. As the FMIs act as nodal points in the processing of payments and securities transfers, IT risks – and more particularly cyber risks – also continue to require the necessary attention. Cyber risks and FinTech are discussed in chapter G below.

Securities clearing, settlement and custody

Although there is no Belgium-based central counterparty (CCP) involved in securities clearing, the Bank participates in various CCP supervision colleges, either because those institutions settle transactions on the books of a Belgian Central Securities Depository (CSD), or because of the importance of a Belgian financial institution as a CCP participant. Since the euro-denominated activities of CCPs currently operating from the United Kingdom may be significant, the impact of Brexit is being closely monitored.

(1) See <https://www.nbb.be/doc/ts/publications/fmi-and-payment-services/2017/fmi-report2017.pdf>.

TABLE 28 MAPPING OF THE FINANCIAL MARKET INFRASTRUCTURES AND PAYMENT SERVICES SECTOR

	International cooperation		The Bank acts as the sole authority
	The Bank acts as lead authority	That Bank participates under the direction of another authority	
Prudential supervision		<u>Securities depository</u> Bank of New York Mellon SA (BNYM SA/NV)	<u>Securities depository</u> BNYM Brussels branch
			Payment service providers (PSP) ⁽¹⁾ Payment institutions (PI) Electronic money institutions (ELMI)
Prudential supervision and oversight	<u>Securities settlement systems</u> <u>Securities depository (CSD)</u> Euroclear Belgium (ESES) <u>International securities depository (ICSD)</u> Euroclear Bank SA/NV <u>Equivalent settlement institution</u> Euroclear SA/NV (ESA)	<u>Securities clearing systems (CCP)</u> LCH.Clearnet Ltd (UK), ICE Clear Europe (UK), LCH.Clearnet SA (FR), Eurex Clearing AG (DE), EuroCCP (NL), Keler CCP (HU), CC&G (IT)	
			<u>Payment processors</u> Worldline SA/NV
Oversight	<u>Critical service provider</u> SWIFT	<u>Critical service provider</u> TARGET2-Securities (T2S)	<u>Securities settlement systems</u> <u>Securities depository</u> NBB-SSS
		<u>Payment system</u> TARGET2 (T2) CLS Bank	<u>Card payment schemes</u> Bancontact MasterCard Europe
			<u>Payment system</u> Centre for Exchange and Clearing (CEC)

Post-trade infrastructure	<u>Securities clearing</u>	Payments	Payment systems
	<u>Securities settlement</u>		Payment institutions and electronic money institutions
	<u>Custody of securities</u>		Payment processors
Critical service providers	TARGET2-Securities		Card payment schemes
	SWIFT		

Source: NBB.

(1) For a list of payment service providers, see <https://www.nbb.be/doc/ts/publications/fmi-and-paymentservices/2017/2017-chapter-3-2-payment-institutions-electronic-money-institutions.pdf>.

In the CSD sector, the implementing and regulatory technical standards of the CSD Regulation⁽¹⁾ came into force on 30 March 2017. The Regulation defines the common rules on settlement in the EU, regulates the activities performed by CSDs, organises the provision of banking services related to CSD activities, and deals with sanctions and the deadlines for obtaining authorisation to perform

the functions of a CSD. Every CSD in the EU must apply to its competent authority for authorisation.

As the competent authority in Belgium, the Bank authorises and supervises CSDs established in Belgium. The Bank seeks the FSMA's advice for aspects that fall under the latter's limited competence for CSDs as part of its tasks of ensuring compliance with rules guaranteeing the sound operation, integrity and transparency of financial instruments markets, as well as its work on ensuring

(1) Regulation (EU) No. 909/2014 on improving securities settlement in the European Union and on central securities depositories.

compliance with the rules for protecting the interests of investors in financial instrument transactions⁽¹⁾. A protocol setting out the cooperation arrangements was concluded between the two institutions in 2017.

Under the Regulation, the competent authority has to decide on the completeness of the application for authorisation. Applications for authorisation submitted by CSDs based in Belgium and forming part of the Euroclear group – notably Euroclear Belgium and Euroclear Bank – were considered incomplete for various reasons, such as the non-exhaustive character of the application, ongoing IT changes, and the incomplete implementation of new control processes and procedures. Euroclear Belgium and Euroclear Bank must provide all the additional information for assessing their compliance with the Regulation's requirements by no later than the end of September and the end of December 2018 respectively. From the moment the application is considered complete, the Bank, as the competent authority, will transmit all the necessary information to the other authorities which, pursuant to the Regulation, have to be consulted on the conformity of the application. BNY-Mellon CSD decided not to submit an application for authorisation.

The Regulation exempts NBB-SSS, like other public CSDs, from certain obligations, such as obtaining an authorisation. However, these CSDs must comply with all other obligations applicable to them by no later than one year from the date of entry into force of the technical standards, i.e. by 30 March 2018 at the latest.

In view of the importance of the entities located in Belgium internationally active in securities settlement, custody and related services on behalf of professional clients, the prudential supervision approach applied to this sector in Belgium was adapted to the specific character of those activities long ago. In order to optimise this approach, it was considered appropriate to introduce an additional supervision status specifically geared to banking entities operating exclusively in the custody and servicing of securities.

The main activity of these entities in fact consists in holding financial instruments off the balance sheet for their clients. However, the banking regulations do not address prudential supervision aspects relating to such activity;

it is therefore justifiable and necessary to apply a special prudential supervision approach to these institutions for the relevant aspects which are not covered by the banking regulations.

Technically, the current definition of “assimilated settlement institutions” is divided into two sub-categories in order to include credit institutions based in Belgium whose activity consists solely in providing their clients with securities custody services, accounting and settlement of financial instruments, and ancillary services.

These institutions are in fact very similar to existing assimilated settlement institutions, defined as entities which deal with all or part of the operational management of services provided by settlement entities. Those similarities are in particular as follows: the type of activities pursued, the absence of retail deposits and other retail customer services, such as retail lending, and the maintenance of the risk profile at a low level. The Law introducing this new type of authorisation came into force on 21 August 2017⁽²⁾.

Payments

The Bank bears wide responsibility for payments and – depending on the system or the institution – acts as the overseer or the prudential supervision authority. As the overseer, the Bank covers payment systems, payment instrument processors and card payment schemes, while, as the prudential supervisory authority, it supervises payment service providers.

The proper, secure processing of card payments in Belgium is a key aim of the Bank's oversight, in view of the role of such payments in the economy. Although payment processors are not necessarily payment systems, the Belgian economy is heavily dependent on their smooth operation, and hence on the stability and continuity of card payments. The Law of 24 March 2017 on the supervision of payment transaction processors makes systemically important payment processors subject to the direct legal supervision of the Bank, and lays down certain conditions for pursuit of the activity⁽³⁾.

At the end of 2017, 19 payment institutions and 5 electronic money institutions were subject to the Bank's supervision. The Bank also exercised supervision over eight exempt legal entities and three branches of foreign institutions. During the year under review, four Belgian payment institutions were authorised, including MoneyGram and Ebury Partners which, in view of Brexit, decided to establish a subsidiary in Belgium, while one authorisation was withdrawn. All these institutions

(1) The rules on conflicts of interest, record-keeping, the requirements concerning participation, transparency, procedures for communicating with participants and other market infrastructures, the protection of the assets of participants and of their clients, freedom to issue securities via any CSD authorised in the EU, and access between a CSD and another market infrastructure.

(2) Law of 31 July 2017 concerning miscellaneous financial and fiscal provisions and measures relating to concession contracts.

(3) Law of 24 March 2017 on the supervision of payment transaction processors.

TABLE 29 NUMBER OF PAYMENT AND ELECTRONIC MONEY INSTITUTIONS SUBJECT TO SUPERVISION

(end-of-period data)

	2014	2015	2016	2017
Payment institutions	18	20	24	26
Under Belgian law	11	12	16	19
Exempt institutions ⁽¹⁾	4	5	5	5
Branches governed by the law of an EEA member country	3	3	3	2
Electronic money institutions	11	11	9	9
Under Belgian law	5	5	5	5
Exempt institutions ⁽¹⁾	5	5	3	3
Branches governed by the law of an EEA member country	1	1	1	1

Source: NBB.

(1) "Exempt institutions" are subject to a lighter supervision regime in accordance with Circular NBB_2015_12 on the Bank's exemption policy on the basis of Article 48 of the Law of 21 December 2009.

endeavour to offer their services in totally digital form by taking advantage of innovations in financial technology (see also chapter G.3 on FinTech).

During the period under review, one of the priorities of the prudential supervision of payment institutions and electronic money institutions concerned the transposition of the second European Payment Services Directive (PSD2)⁽¹⁾. That Directive, which concerns recent innovations in payment services and for which the Belgian transposition law came into force at the beginning of 2018, adds two new categories of payment services providers to the regulatory framework: payment initiation service providers and account aggregation service providers. These two types of service providers will be entitled, in the same way as other institutions authorised for that purpose, to gain access to the payment accounts of a payment services user provided the user has explicitly given consent. One of the possible applications of this change in the legal framework is the option for an account aggregation service provider to set up a single application containing the balance of the various accounts that an individual holds with multiple financial institutions. As regards payment initiation service providers, the new regime enables them to initiate payments directly from a user's payment account to a payee.

The supervision regime applicable to each type of payment service provider is proportionate to the scale of the providers' activities and the associated risks.

Another key element of the PSD2 is the application of "strong authentication" of the customer with a view to the totally secure initiation and execution of payments. This type of authentication requires the use of at least two of the following three elements, which must be independent and confidential: an element known only to the user (e.g. a PIN code), an element held only by the user (e.g. a payment card) and an element specific to the user (e.g. biometric data, such as a fingerprint).

With a view to uniform application of the new regulations in the EEA, the EBA is to draw up technical standards on the subject.

Provision of critical services

SWIFT (Society for Worldwide Interbank Financial Telecommunication) is a limited liability cooperative society based in Belgium and specialising in the exchange of financial messages between financial institutions and financial market infrastructures.

SWIFT is neither a financial institution nor a financial market infrastructure, but operates as a critical service provider for each of those parties, and is therefore itself systemic. That is why SWIFT is subject to international cooperative oversight exercised by various central banks. The Bank takes on the role of lead overseer for SWIFT and, in that capacity, cooperates with the G10 central banks⁽²⁾. The conclusions of these oversight activities are also

(1) Directive (EU) 2015/2366 of the European Parliament and of the Council, of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No. 1093/2010, and repealing Directive 2007/64/EC.

(2) Bank of Canada, Deutsche Bundesbank, European Central Bank, Banque de France, Banca d'Italia, Bank of Japan, De Nederlandsche Bank, Sveriges Riksbank, Swiss National Bank, Bank of England and the Federal Reserve System, represented by the Federal Reserve Bank of New York and the Board of Governors of the Federal Reserve System.

shared with a wider group of central banks in the SWIFT Oversight Forum⁽¹⁾. The Bank keeps a particularly close eye on developments in SWIFT and maintains continuous relations with the institution. As the lead overseer, the Bank acts as the central contact point for the cooperative oversight, and chairs the groups in charge of technical activities and the high-level groups responsible for defining the oversight policy. The Bank also provides the supporting secretariat for these activities.

The cooperative oversight is essentially organised around five main themes (a) risk detection and management, (b) data security, (c) the system's reliability and resilience (d) technological developments and planning, and (e) communication with users. For each of these themes, there are high-level expectations in relation to SWIFT.

(1) For the composition of the Forum, see the description at: <https://www.nbb.be/en/financial-oversight/oversight/critical-service-providers>.

(2) CPMI-IOSCO (2016), *Guidance on cyber resilience for financial market infrastructures*, BIS (<http://www.bis.org/cpmi/publ/d146.pdf>).

In 2017, apart from a series of recurring subjects such as monitoring of the effectiveness of SWIFT's internal control system (collaboration between the institution's line managers, risk management and internal audit) or strategic decisions concerning expected technological developments, the Bank devoted due attention to cyber risk (see chapter G.4) and SWIFT's strategic stance on that challenge. A first specific theme examined in the year under review concerned the roll-out of the Customer Security Programme (CSP) and the accompanying SWIFT communication to its users on sound management practices and responsibilities concerning security. In the years ahead, the further development of the CSP will most likely remain a priority for the oversight of SWIFT. A second key aspect of cyber risk concerns the assessment of SWIFT's internal resilience to cyber threats and the associated investment. In that connection, the cyber strategy that SWIFT devises and the procedures which it develops pursuant to that strategy are also analysed in the light of the CPMI-IOSCO guidance on the subject⁽²⁾.