Report

Oversight of cashless payment instruments and financial market infrastructures

2017

BANQUE DE FRANCE

EUROSYSTÈME

CONTENTS

Foreword 5

Introduction 7

Chapter 1: Oversight of financial market infrastructures between 2015 and 2017 9

1. Regulatory developments in the area of financial market infrastructures 9

1.1 Recovery and resolution of central counterparties: a clearer international framework 9

1.2 The proposed review of the European Market Infrastructure Regulation 12

1.3 Amendment of the regulation on systemically important payment systems 12

1.4 Finalisation of the European Central Securities Depositories Regulation 14

1.5 Implementation of new international cyber résilience standards 16

2. Report on oversight of financial market infrastructures 17

2.1 LCH SA 18

2.2 Euroclear France and ESES France 21

2.3 CORE(FR) 23

2.4 SEPA.EU 24

2.5 Cooperative oversight 26

Chapter 2: Oversight of cashless payment instruments between 2015 and 2017 29

1. Regulatory changes in the field of cashless payment instruments 29

1.1 The application of the second European payment services directive 29

1.2 Instant payment: the European Payments Council's SCT Inst scheme 30

1.3 Creation of the *Comité national des paiements scripturaux* 32

1.4 Creation of the *Observatoire de la sécurité des moyens de paiement* 33

1.5 Updating of the cheque security framework 34

1.6 Changes in anonymous prepaid cards 36

Contents

2. Report on oversight of cashless payment instruments 37

2.1 Report on post-SEPA migration 37

2.2 Contribution of the Banque de France to the autorisation procedure for payment and electronic money institutions 38

2.3 Contribution of the Eurosystem's payment card oversight actions 38

2.4 Verification of the security and proper functioning of cheques and online payments 39

2.5 Report on oversight of special paperless payment orders 40

2.6 Oversight of complementary community currencies 42

2.7 Analysis of the risks associated with the development of crypto-assets 42

GLOSSARY 45

BOXES

1 Central counterparties resolution – Financial Stability Board Guidance (5 July 2017) 11

2 Brexit : impacts on market infrastructures 13

3 Strong customer authentication 31

4 Support for the development of FinTechs in the payments field in France 32

5 The nine security objectives of the new cheque security framework 35

6 Legal classification of prepaid cards and due diligence obligations of issuers 36

7 Key security measures introduced by the European Central Bank recommendations in the assessment guide 39

8 Avenues for regulation explored by public authorities 43

Pursuant to Article L141-4 § I and II of the Code monétaire et financier *(Monetary and Financial Code), the Banque de France oversees the:*

- *proper functioning and security of payment systems;*
- *security of systems for the clearing, settlement and delivery of financial instruments;*
- *security of cashless payment instruments and relevance of the applicable standards.*

Proper functioning and security of financial market infrastructures and payment instruments are vital for the entire economy. They enable monetary policy to be implemented effectively and contribute both to financial stability and to users' confidence in the currency.

The Banque de France reports regularly to the public on the performance of its duty to oversee financial market infrastructures and payment instruments. The last report was published in 2014. This report covers the period from 2015 to 2017.

Significant developments occurred in the oversight of financial market infrastructures and cashless payment instruments during the period under review. These changes reflect amendments to the regulatory framework and the emergence of new issues. In this respect, the following points are noteworthy.

• *The continuing transformation of the regulatory environment for the oversight of financial market infrastructures: after an initial phase in 2012-2014 during which the work of the CPMI[1] and the IOSCO[2] was transposed into European regulations under the aegis of the European Union (EU), the last few years have been marked by the European Commission's first review of existing regulations. Of particular note is the revision of the European Market Infrastucture Regulation (EMIR), which addresses, firstly, the clearing and reporting obligations and, secondly, the supervision of third-country central counterparties (CCPs) and EU CCPs. Internationally, work on the recovery and resolution of CCPs has been a major focus of the authorities due to the systemic importance of these infrastructures.*

• *An assessment of the initial consequences of the United Kingdom (UK)'s decision to leave the EU and the European Economic Area: the forthcoming departure of the UK lends particular urgency to the revision of the European supervisory framework for third-country CCPs because it will change the status of British CCPs, which will very likely become third-country CCPs, despite the fact that they provide clearing services for several markets of systemic importance for the EU. In the case of payment instruments, the main issue is the future of the European passport, which entitles British institutions to operate in France, because nearly 400 payment institutions (PIs) and electronic money institutions (EMIs) authorised in the UK operate in France under the rights granted by the European passport (freedom to provide services and freedom of establishment). In contrast, fewer than 20 French PIs and EMIs operate in the UK. This issue also concerns credit institutions, which may be authorised to provide the same services as PIs and EMIs, and the Visa and American Express payment card schemes, whose European operations are conducted from London.*

• *The growing importance of cybersecurity risks: whereas previously the regulatory focus had been on the availability of infrastructures, new requirements concerning data integrity and the overall resilience of the ecosystem (systems, data, processes and persons) have been put forth by various bodies (the CPMI-IOSCO* Guidance on Cyber Resilience for Financial Market Infrastructures, *the Network Information Security (NIS) Directive on the security of network and information systems in the EU, the French* loi de programmation militaire*), which promote a holistic approach involving all financial sector operators.*

• *Security as a major issue in the development of innovative and effective payment instruments, which is a prerequisite to promoting confidence in their use and the acceptance thereof: since 2007, with the adoption of the first European directive on payment services (PSD1), Europe has had a harmonised legal framework for payment services, which focused on payment instruments such as cards, credit transfers and direct debits.*

1 Committee on Payments and Market Infrastructures – *https://www.bis.org/cpmi/*

2 International Organization of Securities Commission – *https://www.iosco.org/*

At the same time, the aim to promote competition in the sector by encouraging new entrants, while ensuring consumer protection, led to the adoption, on 25 November 2015, of the second European directive on payment services (PSD2), which extends the scope of regulated payment services to new services and operators, and tightens the security requirements applicable to payment market operators. This new regulatory framework, in particular the requirement for market operators to adopt strong authentication measures, is consistent with the recommendations made by the Banque de France in this area. At the national level, the French Parliament adopted the Act of 9 December 2016 on transparency, preventing corruption and modernising the economy, which expands the remit of the Observatoire de la sécurité des cartes de paiement *(OSCP –Observatory for Payment Card Security) to all cashless payment instruments (thereby becoming OSMP – the Observatory for the Security of Payment Means). The OSMP performs security analyses that are indispensable for the work performed by the* Comité national des paiements scripturaux *(CNPS – National Cashless Payments Committee), which oversees implementation of the national payments strategy.*

This report is divided into two main chapters, which feature the oversight of financial market infrastructures (Chapter 1) and of cashless payment instruments (Chapter 2). Each chapter first presents the main changes to the oversight landscape since 2015, and then describes the oversight actions undertaken by the Banque de France.

Oversight of financial market infrastructures between 2015 and 2017

As a national competent authority, the Banque de France is tasked with the oversight of the French financial market infrastructures, alongside the *Autorité de contrôle prudentiel et de résolution* (ACPR – Prudential Supervision and Resolution Authority) and the *Autorité des marchés financiers* (AMF – Financial Markets Authority), depending on the infrastructures concerned. It also contributes to the cooperative oversight of various European and international market infrastructures and payment systems.

1| Regulatory developments in the area of financial market infrastructures

A significant development during the period covered by the previous oversight report (2012-2014) was the adoption of European regulations targeting various types of infrastructures that transposed the Principles for Financial Market Infrastructures (PFMI)[1] issued internationally by the CPSS[2] and the IOSCO[3] in April 2012: the European Market Infrastructure Regulation (EMIR) of July 2012 on central counterparties (CCPs) and trade repositories,[4] the 2014 Central Securities Depositories Regulation (CSDR) on securities settlement systems and central securities depositories, and the European Central Bank (ECB) regulation on systemically important payment systems (SIPS), which came into force in 2014.

During the period under review, additional work was carried out internationally on the recovery and resolution of CCPs. This period was also marked by an initial review of the existing regulations adopted in previous years: EMIR is in the process of being amended and CSDR has been supplemented by various delegated regulations (technical standards). In addition, the ECB

Regulation on SIPS was amended for the first time in 2017 to clarify existing requirements and establish new ones.

1|1 Recovery and resolution of central counterparties: a clearer international framework

The recovery of a financial market infrastructure (see CPMI-IOSCO glossary)[5] refers to all measures that enable maintaining the infrastructure as a going concern and continuing the provision of critical services in the event of losses due to the default of a participant or other causes. Implementing recovery measures is the responsibility of financial market infrastructures, which are required to provide for such recovery measures in their internal rules of procedure. In contrast, resolution is initiated and carried out by the resolution authorities, in particular if the recovery phase has failed, and aims to allocate losses, wind down operations in an orderly manner and, if necessary, transfer the operations to a bridge entity.

1 *https://www.bis.org/cpmi/publ/d101a.pdf*

2 Which has since been renamed Committee on Payments and Market Infrastructures (CPMI),– *https://www.bis.org/cpmi/*

3 International Organization of Securities Commissions– *https://www.iosco.org/*

4 Trade repositories are supervised by the European Securities and Markets Authority (ESMA).

5 *https://www.bis.org/cpmi/publ/d00b.htm?&selection=156&scope=CPMI&c=a&base=term*
Recovery includes all actions of a financial market infrastructure, consistent with its rules, procedures and other ex ante contractual arrangements, to address any uncovered credit loss, liquidity shortfall or capital inadequacy, whether arising from participant default or other causes (such as business, operational or other structural weakness), including actions to replenish any depleted prefunded financial resources and liquidity arrangements, as necessary to maintain the financial market infrastructure as a going concern and the continued provision of critical services.

International work on the recovery and resolution of infrastructures has gathered pace since late 2014. In October 2014, the CPMI and the IOSCO published a report on the recovery of infrastructures.[6] In the interest of consistency, the Financial Stability Board (FSB) at the same time adopted additional recommendations on the resolution process in the form of annexes to the Key Attributes of Effective Resolution Regimes,[7] which apply to market infrastructures, including CCPs.

Due to the systemic importance of CCPs and the particular financial issues raised by the recovery and resolution of these infrastructures, specific work has been devoted thereto, focusing on recovery and resolution aspects. The PFMI, followed by EMIR, already provide significant coverage for the financial risks of CCPs, whether such losses are due to a participant default (which are covered by initial margins and default fund contributions) or other types of losses (due to operational, business or investment risks), which are initially covered by the infrastructures' own funds. However, in connection with the policy of the FSB[8] to extend recovery and resolution measures to non-bank systemically important financial institutions, it was deemed necessary to supplement these principles with measures covering all foreseeable crisis scenarios, even if unlikely. These scenarios go beyond the scenarios of extreme but plausible losses used in stress tests to calibrate prefunded resources (margins and default fund contributions) for CCPs.

Therefore, at the international level, in April 2015 a CCP workplan was defined by the FSB, in conjunction with the BCBS and CPMI-IOSCO,[9] which included a section setting out the international principles applicable to the recovery and resolution of CCPs. On 5 July 2017, the FSB published guidance[10] (see Box 1) that had been prepared by a group that included resolution authorities and CCP supervisors. In July 2017, the CPMI and the IOSCO updated their 2014 report on the recovery of financial market infrastructures[11] to take into account developments in international discussions, and published it at same time as the FSB's final guidance.

At the European level, in late November 2016, the European Commission published a proposed regulation on the recovery and resolution of CCPs. The aim of this proposal is to transpose the international standards into European Union (EU) law. The objective of the regulation is to provide a framework for the measures that CCPs adopt in their recovery plans, to grant resolution authorities the powers necessary to resolve a non-viable CCP and to define the resolution tools required to ensure financial stability and continue CCPs' critical services. The objective is to avoid the use of public funds, except as a last resort if all other available tools to allocate losses (cash calls, variation margin haircuts, contract tear-ups, writing down the CCP's equity, etc.) do not absorb all losses. The EU Member States must inter alia designate the resolution authorities for CCPs, which should set up resolution colleges that will be consulted in connection with the approval of CCPs' recovery plans, and that will take part in the process of adopting the resolution plans prepared by the national resolution authorities.

The proposal submitted by the European Commission – on which discussion will continue in 2018 – has developed an approach that is quite similar to that advocated by the French authorities. The Banque de France recommends allowing significant flexibility in the use of resolution tools in order to be able to deal with situations that, by definition, are considered unlikely and are, therefore, difficult to foresee, but that may be of significant consequence in terms of financial stability. The power of resolution authorities to intervene early if necessary is also a significant aspect of the French position that is included in the European proposal. With respect to resolution tools, the rules for allocating potential losses of CCPs that exceed the loss allocation mechanisms of EMIR should only cause CCP participants

6 https://www.bis.org/cpmi/publ/d121.pdf

7 http://www.fsb.org/wp-content/uploads/r_141015.pdf

8 http://www.fsb.org/

9 http://www.fsb.org/wp-content/uploads/Joint-CCP-Workplan-for-2015-For-Publication.pdf

10 http://www.fsb.org/wp-content/uploads/P050717-1.pdf

11 https://www.bis.org/cpmi/publ/d162.pdf

Box 1

Central counterparties resolution – Financial Stability Board Guidance (5 July 2017)

The aim of the Financial Stability Board (FSB)'s Guidance is to establish a standardised international framework that supplements the Key Attributes and facilitates implementing a resolution regime for central counterparties (CCPs).

The guidance stresses that orderly resolution is crucial for maintaining financial stability and continuing critical CCP services. For this purpose, the authorities should have the necessary tools and powers, which should be incorporated into both the national law and CCPs' contractual arrangements and rulebooks in each jurisdiction (i.e. the power to partially or fully terminate contracts, forced allocation of open positions, and the power to allocate losses).

To regulate the exercise of resolution powers, the guidance endorses, firstly, a principle of equity in allocating losses, distinguishing situations due to the default of a clearing member from non-default situations, and, secondly, the principle that creditors should not be worse off in the event of liquidation ("no creditor worse off" (NCWO) safeguard). Therefore, financial resources will be of particular importance for the authorities, which must assess precisely the financial requirements necessary to achieve resolution objectives (resolvability assessments).

The guidance requires that resolution plans be adopted for all systemically important CCPs, in close cooperation between the relevant authorities, in particular:

- between the resolution and supervisory authorities, if they are different, in setting up recovery plans and developing crisis scenarios;

- the resolution authority in the home State should establish a Crisis Management Group (CMG) for CCPs that are systemically important in more than one jurisdiction, which the relevant authorities should use to develop and coordinate their resolution plans;

- processes for cooperation and information sharing should be set up within the CMGs through specific cooperation agreements (CoAgs).

Lastly, the cross-border effectiveness and enforceability of resolution measures must be analysed and assessed by the authorities in light of the contractual, operational and organisational arrangements of systemically important CCPs.

In the summer of 2017, the FSB published a report that included a list of 12 CCPs identified as systemically important in more than one jurisdiction, on the basis of criteria developed by the CPMI-IOSCO, and for which a CMG had been or would shortly be set up.

1 *http://www.fsb.org/wp-content/uploads/P050717-3.pdf*

losses that are quantifiable and manageable in a situation of market turmoil, in accordance with the CPMI-IOSCO 2014 report on the recovery of FMIs. Therefore, the Banque de France feels that certain tools that could be detrimental to financial stability should be avoided. For example, this would be the case for initial margin haircutting, which creates potentially unlimited exposure for participants and imposes significant liquidity restrictions, and also creates incentives for non-defaulting members to leave the CCP if a participant defaults. The forced allocation of positions, which could oblige certain members to take positions that they are incapable of handling, should also be excluded because it increases the financial risks of a resolution.

1|2 The proposed review of the European Market Infrastructure Regulation

The European Commission has made two proposals for revising EMIR. The first one, which focuses on clearing and reporting obligations, aims to promote proportionate implementation of regulatory requirements in this area, whereas the second proposal addresses the oversight of third-country CCPs and EU CCPs.

The first aspect, known as "EMIR REFIT",[12] led to proposals that were published on 4 May 2017, and which call for reducing the burden of certain clearing and reporting obligations, in particular for non financial counterparties, as well as introducing the possibility of temporarily suspending the clearing obligation. Discussions are being finalised with a view to adopting an amended regulation in 2018.

Moreover, on 13 June 2017, the European Commission published a proposed revision of the regulation, known as "EMIR 2", which calls for a restructuring of the supervisory framework for third country CCPs and EU CCPs, by amending the regulation that created the European Securities and Markets Authority (ESMA) and EMIR, which regulates over-the-counter derivatives markets and CCPs.

12 REFIT : Regulatory Fitness and Performance Programme.

The future withdrawal of the United Kingdom from the EU and the change in the status of British CCPs, which will very likely become third-country CCPs, require a revision of the European regulations on third-country CCPs because British CCPs provide clearing services for several markets of systemic importance for the EU. The current third-country CCP recognition arrangements under EMIR are no longer appropriate because they do not provide ESMA with discretion or true supervisory power, despite the fact that certain recognised third-country CCPs are closely interdependent with the EU's financial system. Therefore, the Commission is proposing a proportionate approach that defines differentiated requirements for third-country CCPs depending on their systemic importance for the EU (see Box 2).

In the case of CCPs established in the EU, the national authorities would continue to exercise supervisory powers. An increased role for ESMA would promote enhanced supervisory convergence at the European level. Moreover, the central banks of issue of the currencies in which the CCPs clear transactions would also have increased and binding powers to review the decisions that concern them most directly, pursuant to their duty to implement monetary policy.

1|3 Amendment of the regulation on systemically important payment systems

The regulatory environment for payment systems also underwent a major change with the amendment of the Regulation of the ECB (EU) 795/2014 of 3 July 2014 on oversight requirements for systemically important payment systems (SIPS) which resulted in ECB Regulation 2014/28. This is the first amendment since the publication of the regulation: future amendments will take place every two years. The amendment draws on experience acquired from the supervision of the Eurosystem since the regulation was adopted in 2014, and from consultations with the operators of the four SIPS (TARGET2, EURO1, STEP2-T and CORE(FR)), which were held in December 2016

Box 2

Brexit: impacts on market infrastructures

The decision of the United Kingdom (UK) to leave the European Union (EU) and the European Economic Area (EEA), which will take effect in March 2019, has significant implications for the regulation and supervision of market infrastructures established in the UK. In particular, certain British central counterparties (CCPs) are of significant systemic importance for the remaining 27 Member States of the EU. For example, LCH Ltd clears 95% of the worldwide market in interest rate swaps, including swaps denominated in euros and five other EU currencies, as well as about 30% of the repo market cleared in euros and ICE Clear Europe Ltd clears LIFFE, a market for short-term interest rate derivatives, and holds a majority position in the EU in the clearing of credit default swaps (CDS).

Currently, these CCPs are subject to European Market Infrastructure Regulation (EMIR), which imposes prudential requirements that exceed international standards, and are supervised by the Bank of England. The Bank of England chairs the supervisory colleges required by EMIR, which include the European authorities with a primary interest therein, including the *Autorité de contrôle prudentiel et de résolution* and the *Autorité des marchés financiers* for the supervision of French clearing members, and the European Central Bank as the central bank of issue for the euro. After the United Kingdom leaves the EU and the EEA, these CCPs will be subject to British rules and their EMIR colleges will cease to exist. They will become third-country CCPs, subject to an equivalence regime that is currently not very demanding for the relevant CCPs and their domestic supervisors.

To remedy these deficiencies, on 13 June 2017, the European Commission published a proposal to overhaul the regulation and supervision of third-country CCPs, which gives added powers to European Securities and Markets Authority (ESMA) and the central banks of issue with respect to the recognition of third country CCPs. The proposed arrangement would calibrate the supervision regime applicable to CCPs based on their systemic importance for the EU:

- for non-systemically important CCPs, the current recognition arrangement based on the equivalence of regulatory frameworks will be retained, but will be reviewed regularly and will impose conditions to ensure actual equivalence;
- systemically important CCPs will be obliged to strictly comply with the requirements of EMIR, which will be directly verified by ESMA supervision, as well as with the rules imposed by the central banks of issue within the scope of their responsibilities;
- if certain clearing activities are deemed of particular systemic importance for the EU, the Commission would be empowered to refuse recognition, on the recommendation of ESMA and with the agreement of the relevant central banks (which would require the CCP to relocate to the EU).

These provisions are based on a certain number of observations drawing on past experience.

- A CCP that executes transactions denominated in euros or in another European Union currency, but that is not primarily supervised by a EU authority, may take measures, or be required to take measures by its national supervisory authority, that are not in the interest of the EU's financial stability. This lesson was learnt from past experience, in particular during the euro zone sovereign debt crisis.
- The prospect of Brexit and the abandonment of the European regulatory framework for British CCPs highlight the need to relocate to the EU the clearing of instruments denominated in EU currencies and that are of strategic importance for implementing monetary policy, financing the economy and ensuring financial stability in the zone.

Therefore, the Banque de France strongly supports this initiative, which will provide the European authorities with the means to carry out their duty to protect the financial stability of the EU by ensuring that third-country CCPs that wish to provide services in the EU comply with European requirements.

and February 2017.[13] The amended regulation was published on 16 November 2017. The amended regulation clarifies existing obligations, adds new requirements with respect to risk management and expands the powers of the authorities.

For example, the amended regulation strengthens the governance framework for SIPS by introducing an independent director and providing guidance on the required clear separation between operational, risk management and internal audit functions. The requirements in terms of the board of directors' involvement in and responsibility for decisions that have an impact on the risk profile of the system have also been tightened.

With respect to risks, the amended regulation clarifies the requirements relating to the coverage of financial risks, in particular liquidity risk, and supplements general business risk management obligations. In this regard, the regulation requires that assets held to cover general business risk be segregated from assets used for daily operations, and makes a distinction between (i) payment systems' recovery plans and orderly wind-down plans and (ii) recapitalisation plans. Furthermore, the amended regulation includes additional provisions on custody, investment and operational risk management. With respect to the latter risk, the amended regulation imposes requirements to mitigate cyber risks, which follow the CPMI-IOSCO guidance on the cyber resilience of financial market infrastructures (see Section 1|5). Operators are now required to regularly submit documentation to the regulator about their management of cyber risks, describing governance, identification, protection and detection, and resilience-testing measures.

Operators must comply with these new requirements within 18 months in the case of financial obligations, and 12 months in the case of all other provisions.

Lastly, the competent authorities are granted powers to require corrective measures, and the ECB is granted the power to impose sanctions. The amended regulation also includes a methodological notice that describes the procedure for calculating financial sanctions, as well as the amendment to ECB Regulation 2157/1999 on sanctions.

13 *http://www.ecb.europa.eu/ecb/legal/pdf/celex_32017r2094_fr_txt.pdf*

1|4 Finalisation of the European Central Securities Depositories Regulation

European Regulation 909/2014 on improving securities settlement in the EU and on central securities depositories (commonly called the Central Securities Depositories Regulation – CSDR) was adopted on 23 July 2014. It transposes into European law the PFMI applicable to these infrastructures, with some modifications.

Although the PFMI consider that central securities depositories (CSDs) do not necessarily perform securities settlement functions, CSDR, in contrast, closely links CSDs and securities settlement systems. Under CSDR, a central securities depository must operate a securities settlement system to be classified as a CSD, and must provide at least one of the other two core services defined by CSDR (i.e. notary service and/or maintaining securities accounts at the top tier level). Moreover, in Europe, CSDs are the only entities allowed to operate securities settlement systems, besides central banks that act as CSDs.

Harmonised prudential rules are now applicable for all risks to which CSDs are exposed (in particular, legal risk, operational risk, etc.). The risk management frameworks should enable CSDs to identify, manage and control the risks to which they are exposed, including in the case of operations that are outsourced, which must remain under the CSDs' supervision. Methods for calculating own funds requirements have been defined. Own funds should enable CSDs to cover the risks to which they are exposed, but also to enable their winding-down or orderly restructuring over a period of at least six months. In practical terms, this requires CSDs to be able to pay operating costs over a period of at least six months.

CSDR also introduces harmonised provisions on the functioning of securities markets, in particular: making the dematerialised form (which has been effective in France since 1984) and the immobilisation of instruments standard practice; standardising the settlement cycle, which is now a maximum of two business days between the trading day and the settlement date for transactions traded and executed on a trading venue; and stricter market discipline measures intended to limit settlement fails due to a lack of securities and/or cash (preventive suspension measures, applying financial penalties if delivery occurs after the agreed settlement date, and imposing buy-ins if the delay exceeds four days or seven days depending on the instrument).

Lastly, CSDR aims to remove barriers to the functioning of the post-trade sector in Europe, which remains "fragmented along national lines". Two important measures should contribute to achieving this objective. Firstly, issuers will be able to issue their securities within the European CSD of their choice, and no longer necessarily within the national CSD, subject to compliance with certain provisions of the law of their home country. Although this possibility was available before CSDR was adopted, it was little used in practice. By explicitly providing for this possibility, CSDR intends to open up the business of "issuer CSD" to greater competition between EU CSDs. This should make it possible to choose the CSD(s) that is (are) in the best position to manage issuers' securities efficiently. Secondly, CSDR requires CCPs and trading venues to grant CSDs, upon request, transparent and non-discriminatory access to their transaction feeds, for which they may charge a reasonable commercial fee. CCPs and trading venues will no longer be able to refuse such access, unless it would expose the relevant CCPs and venues to excessive risk.

Although CSDR officially entered into force on 17 September 2014, it applies progressively only as from end-2017. Certain delegated regulations that supplement CSDR with technical measures (in particular, measures concerning operational, authorisation and supervisory requirements applicable to central securities depositories) were only adopted in early 2017 by the European Parliament and the Council, and were then published in the *Official Journal* of the European Union on 10 March 2017. Moreover, according to the most recent information available, specific market discipline measures will be published in delegated regulations supplementing CSDR with technical implementing measures in early 2018. These measures will come into force about two years after they are published, meaning that the market discipline measures will be effectively implemented in early 2020.

Most European States have designated just one competent authority to implement CSDR, which in the vast majority of cases is the financial markets authority. A few States have designated two competent authorities. This is the case in France, which has designated the *Autorité des marchés financiers* (AMF) and the Banque de France. The AMF is competent to grant authorisations, after consulting the Banque de France. The Banque de France has primary jurisdiction in certain areas, such as settlement finality, cash settlements, links between CSDs, operational risk and investment policies. "Relevant authorities" also participate in the authorisation process, in particular the central bank of issue (the Eurosystem in the case of CSDs settling in euros, which will be represented by the national central bank of the jurisdiction in which the various CSDs are established). They may provide non-binding opinions to the competent authority(ies) of a CSD on matters they deem pertinent.

When the regulatory technical standard (RTS) on authorisation came into force on 30 March 2017, existing European CSDs were given a six-month period to submit their CSDR authorisation applications, meaning that the deadline for CSDs to submit their applications to their competent authority(ies) was 30 September 2017. This was

the case for Euroclear France, the only CSD that currently operates in France.

During the authorisation process, existing European CSDs are covered by a grandfather clause that allows them to continue to offer all services listed in CSDR, including the "core services" that the European regulation expressly limits to CSDs. However, if at the conclusion of the process authorisation is refused, they must cease offering the services they previously provided, in particular the operation of their securities settlement system(s). Newly created CSDs must be authorised under CSDR before they commence operations, in particular operating a securities settlement system.

After a CSD submits an authorisation application, the competent authorities have 30 business days to determine if it is complete. If the application is deemed complete, the competent authorities have a non-extendable six-month period to grant or refuse authorisation to the CSD, during which they may request that the CSD submit any additional information that may be necessary to obtain authorisation. However, if the application is deemed incomplete, the relevant authorities must inform the CSD and set a deadline for it to submit the additional information required.

Article 75 of CSDR provides that the European Commission must review and prepare a report on CSDR by 18 September 2019.

1|5 Implementation of new international cyber resilience standards

The proper functioning of financial market infrastructures is vital due to their links to the real economy and the significant interconnections between financial ecosystems. Data that can be accessed from multiple entry points and the speed at which information can be transmitted and data can be processed have significantly contributed to improving the efficacy of financial market infrastructures, by reducing costs while increasing volume-handling capacities. At the same time, these changes have also transformed the nature of risks, and the security of information systems, which was the paradigm in the 2000s, has acquired a new dimension in the 2010s and become cybersecurity. Before the 2000s, cybersecurity issues focused essentially on data protection. The scope broadened ten years later to include detection, ex-post analysis and resolution of cyber-attacks.

Awareness among financial sector operators of the reality of the dangers and impacts of cyber risks reached a high point in March 2016 as a result of the attack suffered by the Bangladesh central bank.

In this new context, the approach of supervisory authorities to cyber risks has evolved fundamentally. For many years, regulatory action focused primarily on the availability of infrastructures, and then on data integrity. Currently, the concept of overall resilience supplements these requirements, and calls for protection of critical functions and data enabling securities clearing, payment and delivery transactions to be executed within the prescribed deadlines. Therefore, cyber resilience is not limited to technological issues, but now extends to systems and data, as well as to persons and processes.

In light of the fact that cyber threats have become a major security and resilience issue for the financial ecosystem, in 2016, the G7 member countries published the *G7 Fundamental Elements of Cybersecurity for the Financial Sector*.[14] This non-binding document has served as the foundation for development of harmonised national strategies for the entire financial sector, including banks and other financial institutions. It sets out eight key elements for managing cyber risks: risk management strategy and framework, governance, risk assessment and control, continuous risk monitoring, responses to cyber incidents, recovery after a cyber incident, information sharing and continuous learning.

International oversight standards do not specifically cover cyber risks, to which financial market

14 *G7 Fundamental Elements of Cybersecurity for the Financial Sector*

infrastructures in particular are exposed. The issue is addressed in a non-specific manner only in relation to the management of operational risk (Principle 17 of the PFMI published in 2012 by CPMI-IOSCO). As cyber-attacks grew in number and sophistication in the 2010s, and as financial market infrastructures and payment systems came to be seen as vectors for rapid contagion within the financial sector, a working group of central banks, financial supervisors and international organisations was tasked with preparing specific cyber risk international standards to supplement the PFMI.

This work, which began in late 2014, culminated in proposed standards in 2015, which were then submitted for public consultation between November 2015 and February 2016. The *Guidance on Cyber Resilience for Financial Market Infrastructures*[15] was then published by CPMI-IOSCO in late June 2016. This document now serves as the reference for the work undertaken by market infrastructures and their supervisory authorities to increase cyber resilience. The Guidance is structured around five main issues: governance, identification, protection, detection and response and recovery. They are supplemented by aspects focusing on culture and situational awareness, training and cyber testing (e.g. intrusion testing of systems), which are concepts that were not systematically covered in prior standards.

At the European level, after three years of negotiations, the work undertaken by the Commission resulted in the publication, on 19 July 2016, of the directive on the security of network and information systems, which is known as the "NIS Directive". The Member States must transpose this directive into their national law by May 2018.

In France, specific requirements for the financial sector were adopted early, as of 2013, in connection with the implementation of the *loi de programmation militaire*,[16] compliance with which is verified by the *Agence nationale pour la sécurité des systèmes d'information* (ANSSI – National Information Systems Security Agency).

Publication of the *Guidance on Cyber Resilience for Financial Market Infrastructures* and the occurrence of a major cyber-attack on the financial system made it a priority, for supervisors and infrastructure operators, to improve the sector's overall level of cyber resilience and, in particular, to mitigate the "weakest link" effect and the general impact of incidents.

The Eurosystem is using the CPMI-IOSCO *Guidance* as the basis for the assessment it has undertaken of the cyber resilience of European payment systems and financial market infrastructures, with a view to strengthening such resilience. This work is focusing on two areas.

- Promoting dialogue between regulators and industry: the European Cyber Resilience Board is a strategic high level forum between regulators and industry representatives on the topic of the cyber resilience of financial market infrastructures and critical service providers. The objective of this forum is to create a dialogue interface, increase awareness of cyber security issues among regulators and the entities they supervise, and promote and strengthen joint initiatives aimed at improving the cyber resilience of the sector.

- Creating a harmonised framework for conducting testing, *such as red-teaming*: this work, which was begun in 2017, will lead to the publication of guides for use by the authorities and operators and by the specialised companies whose services they will use to carry out these sensitive operations.

2| Report on oversight of financial market infrastructures

As a national authority, the Banque de France, along with the ACPR and the AMF, depending

15 *Guidance on Cyber Resilience for Financial Market Infrastructures*

16 *https://www.legifrance.gouv.fr/*

on the infrastructures in question, oversees the financial market infrastructures that operate in France: the central counterparty LCH SA, the central securities depository Euroclear France, the French payment system CORE(FR) and the pan-European payment system SEPA.EU. It also contributes to the cooperative oversight of various payment systems, market infrastructures and critical service providers established in other countries and/or with a pan-European or international scope.

2|1 LCH SA

Activity

Since 11 April 2016, the French central counterparty (CCP) operates under the trade name LCH SA (formerly LCH Clearnet SA, registered under the company name "*Banque centrale de compensation*"). The French CCP offers clearing services for financial instruments, and ensures proper execution of transactions, in four business lines:

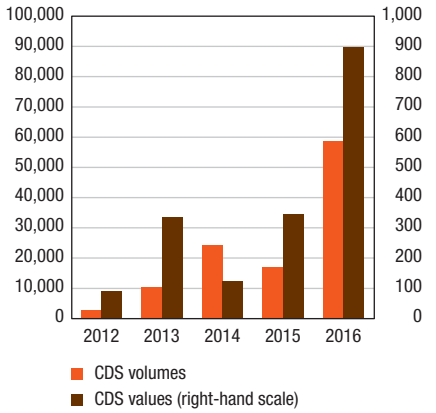
- cash products: cash equities and convertible bonds listed on Euronext markets;
- listed derivatives: equity and commodity derivatives listed on Euronext markets;
- outright trades and repos in government securities: Italian, French, German, Belgian and Spanish sovereign debt securities. This business line includes €GC Plus, a repo clearing service for which collateral is managed on a triparty basis by Euroclear France;
- OTC-traded euro- and USD-denominated credit default swaps (CDS) based on indices or single reference entities.[17]

Recent changes and development projects

In 2017, LCH SA continued and expanded its offer of clearing services in the cash and derivatives segment for the Euronext regulated market.

C1 LCH SA : credit derivatives (CDS)

(volumes in thousands of transactions, values in EUR billions)



Source: Bank for International Settlements (BIS), *Statistics on payment, clearing and settlement systems in the CPMI countries* (*Red Book* – 2017).

In early August 2017, LCH SA and Euronext reached an agreement whereby the French CCP will continue clearing derivatives markets for a renewable ten-year period. That agreement was signed on 31 October 2017. In the cash equities segment, LCH SA also continues to be the main CCP providing clearing services for Euronext markets. However, in late 2016, Euronext decided to open this activity to competition and amended its rulebook to enable participants to choose to have their spot contracts cleared by EuroCCP or LCH SA (preferred CCP model).

In addition, these changes led to the acquisition of equity stakes in partner CCPs. For example, Euronext acquired a 20% stake in the Dutch CCP EuroCCP. Its 2.3% stake in LCH Group Ltd was converted into an 11.1% stake directly in LCH SA. The LSE Group and Euronext also reached agreement on granting Euronext a right of first refusal in the event of a sale of LCH SA, which may be exercised under certain conditions, in particular if the LSE Group decides to sell more than 50% of LCH SA's capital.

17 Cleared index CDS include iTraxx Europe Main, iTraxx Europe Crossover, iTraxx Europe HiVol, CDS iTraxx Europe Senior Financials, CDX North America Investment Grade and CDX North America High Yield. Since late 2017, the CCP also clears options on iTraxx Europe Main and Crossover index CDS.

Furthermore, during the period under review, LCH SA undertook several important initiatives in conjunction with Euronext, such as, in 2015, launching AtomX (a new service developed by Euronext to record trades negotiated outside the order book) and the clearing of various new instruments (single stock dividend futures, futures on wood pellets for the residential market) and, in 2016, the clearing of nitrogen fertiliser derivatives.

During the period, the clearing business in the fixed income segment (debt securities and repos) saw a diversification of the clearing offer for euro-denominated European sovereign debt. LCH SA began clearing German and Belgian sovereign and similar debt (on 27 February and 29 November 2017, respectively), and plans to continue to diversify its clearing offer to other main euro-denominated European sovereign debt.

In the CDS clearing business, the French CCP continued its rapid growth and recently expanded the range of products cleared, successively launching:

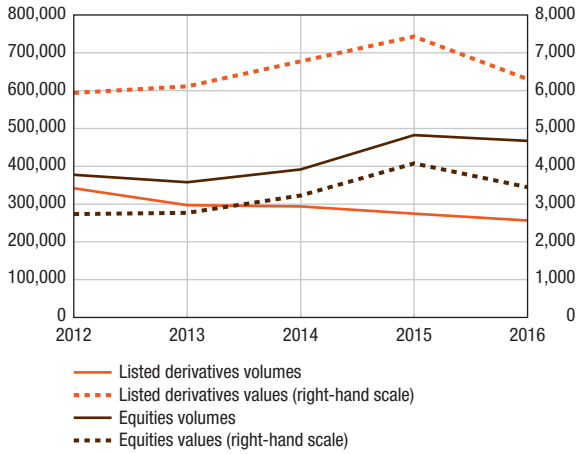
- senior financials CDS (indices and single names), in 2015;
- CDS on USD-denominated US indices and single names (CDX North American Investment Grade Index in March 2016, CDX High Yield Index in December 2016);
- CDS index options in 2017 (iTraxx Europe and iTraxx Crossover 5-year European indices).

In addition, LCH SA's CDSClear segment expanded its market share, with LCH SA's clearing services for these products now accounting for about 20% of euro-denominated CDS cleared in Europe.

Lastly, in early 2017, LCH SA launched the Group Member Access project, which grants its clearing members access to LCH SA's clearing applications over a unique technical solution developed in common with its sister company, LCH Ltd.

C2 LCH SA : spot contracts and equity derivatives

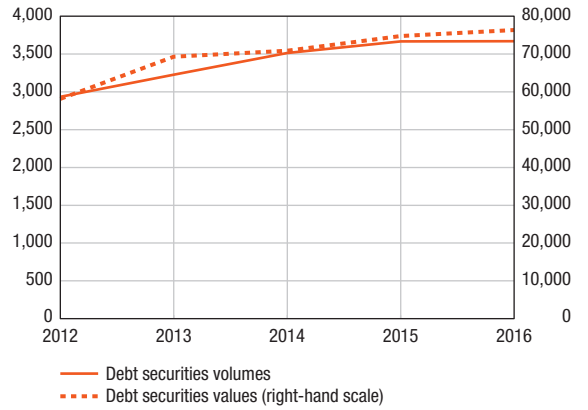
(volumes in thousands of transactions, values in EUR billions)



Source: Bank for International Settlements (BIS), *Statistics on payment, clearing and settlement systems in the CPMI countries* (*Red Book* – 2017).

C3 LCH SA : outright trades and repos in government securities

(volumes in thousands of transactions, values in EUR billions)



Source: Bank for International Settlements (BIS), *Statistics on payment, clearing and settlement systems in the CPMI countries* (*Red Book* – 2017).

The project to rationalise IT applications is expected to continue as part of a transformation plan.

Assessment

The competent national authorities for the CCP are the Banque de France, the ACPR and the AMF, which exercise joint supervision pursuant

to EMIR. LCH SA also has credit institution status and, as such, is supervised by the ACPR, and is classified as a "less significant institution" for Single Supervisory Mechanism purposes.

The competent national authorities use a variety of assessment methods in performing their duty to supervise the central counterparty. The most frequent and customary method is a records-based assessment by the authorities. It consists of reviewing proposals/changes the central counterparty is planning on the basis of documents submitted to the authorities, regular oversight meetings or meetings dedicated to specific projects.

In addition to off-site assessment, the authorities may conduct on-site inspections. The last Banque de France inspection on LCH SA's premises was conducted from November 2015 to May 2016 and focused on the liquidity risk management system. The aim of this inspection was to assess the robustness of its liquidity risk management system, which is an essential aspect for this CCP due to its authorisation as a central counterparty under EMIR, independently of the facilities offered by its credit institution status. More specifically, the inspection team focused on aspects such as governance and internal control, operational management of liquidity, operational management of defaults, the stress-testing mechanism, and liquidity management in the context of its relationship with the Italian central counterparty CC&G, with which LCH SA has established interoperability arrangements. In early 2017, a follow-up letter to the inspection was sent to the CCP, addressing a certain number of corrective measures to be implemented in order to strengthen its liquidity risk management system. The corrective actions have been incorporated into the supervision plan adopted by the French authorities and are monitored regularly.

Pursuant to EMIR, the national authorities include other European national authorities with an interest in the proper functioning of the central counterparty in the oversight of this infrastructure. The participation of these national authorities is defined in EMIR (Article 18). An EMIR college comprises, firstly, the competent national authorities that oversee the central counterparty, but also includes the oversight authorities of entities that the CCP's activities may impact, i.e. the supervisors of the main clearing members, trading venues, CCPs with which interoperability arrangements have been established, central securities depositories, the central banks of issue of the main EU currencies cleared, as well as the ESMA, which does not hold a voting right.

The aim of this system is to promote a standardised approach to implementing EMIR requirements in the EU and an appropriate assessment of the CCP's risks, taking into account its risk profile and the various market segments it clears, while involving the main relevant authorities of other EU member countries. The college of authorities is the appropriate forum for exchanging information about the CCP and studying changes the CCP proposes. LCH SA's EMIR college was set up in January 2014 and comprises 19 authorities (including ESMA) from 9 different EU countries. The Banque de France chairs the college. College meetings provide an opportunity for exchanging various types of information with other authorities on the supervisory assessment for the past year and to inform them of the supervision plan and the topics that the national authorities have decided to study in greater depth, in addition to the proposals/changes submitted for their review.

In accordance with EMIR, the opinion of the college is required, expressed by a vote as provided in Article 19 of EMIR, when a CCP is authorised, but also on proposals to expand service offers, initiate new business lines and matters that have a material impact on the CCP's risk management system, such as a change to its margin model.

The French authorities scheduled four meetings of the college between 2015 and 2017. The college meets at least once a year after having reviewed

relevant matters, and other meetings may be convened on specific issues or in the event of a crisis.

2|2 Euroclear France and ESES France

Activity

Euroclear France, the central securities depository established in France, offers the three "core services" defined by CSDR[18]: a notary service for the issuance of securities, a central maintenance service for securities accounts, and a securities settlement service to enable the circulation of securities. In addition to these three core services, Euroclear France offers various "ancillary" services, such as managing securities transactions (payment of coupons and dividends, etc.), tripartite collateral management, assigning an ISIN code to new securities issued, etc.

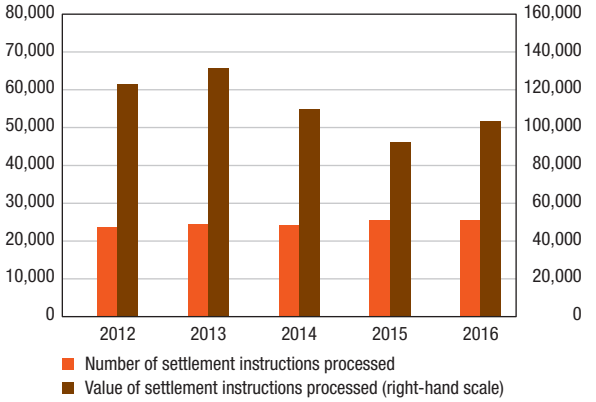
Euroclear Settlement of Euronext-zone Securities (ESES) France is the French securities settlement system (SSS), which has been connected to TARGET2-Securities (T2S) since 12 September 2016. Currently, nearly all securities transactions and trades are processed on T2S, to which Euroclear France outsources the securities settlement service. French institutions that have a direct access to the securities settlement system have a contractual relationship with Euroclear France only, whether they are technically T2S "directly connected parties" or "indirectly connected parties", and they have no contractual ties with T2S.

Since 2010, the Belgian and Dutch CSDs have outsourced operational management of their securities settlement business to Euroclear France.

ESES France processes about 90% of the securities settled by the three ESES CSDs. Based on the data of the European Central Securities Depositories Association (ECSDA),[19] about 12% of European securities are in custody with Euroclear France, and somewhat less than 10% of securities transactions settled in Europe are settled by Euroclear France. The value of securities in custody increased by about 3% in 2016 to EUR 6,300 billion, whereas the value of settlement instructions increased even more rapidly, by about 12%, to around EUR 103 trillion (See Chart 4).

C4 Settlement instructions processed by ESES France

(volumes in thousands of transactions, values in EUR billions)



Source: Bank for International Settlements (BIS), *Statistics on payment, clearing and settlement systems in the CPMI countries* (*Red Book* – 2017).

Recent changes and development projects

On 12 September 2016, Euroclear France successfully migrated to T2S, the pan-European securities settlement platform, in the third migration wave. This successful migration completed a significant process to adapt operationally and legally to this harmonised environment. The preparation for this migration, which required, in particular, increasingly complex tests involving ever larger numbers of stakeholders, was closely monitored by the Banque de France and the AMF in 2015 and 2016.

The vast majority of European CSDs (except Euroclear Bank and Clearstream Banking Frankfurt) have migrated to T2S, in particular the Italian CSD, Monte Titoli, which joined T2S during the first migration wave in June 2015.

18 See Section 1|4 for additional details.

19 *https://ecsda.eu/*

The German CSD Clearstream Banking Frankfurt joined the platform in February 2017 during the fourth migration wave. Euroclear France, which had established two relayed links to these CSDs (in which Euroclear Bank acted as intermediary CSD), converted them into "internal T2S" direct links and, therefore, can now offer its participants delivery versus payment (DvP) real-time settlement of securities issued or held in Germany and Italy, in the same manner as domestic transactions in securities issued in France, and for the same price.

Assessment

The ESES securities settlement systems and CSDs (Euroclear France, Euroclear Nederland and Euroclear Belgium) are overseen under a cooperation arrangement between the French, Belgian and Dutch authorities responsible for overseeing and regulating the central securities depositories and securities settlement systems of the Euroclear group. A memorandum of agreement entered into in July 2011 defines the procedures applicable to their cooperation and information exchanges with respect to regulation and supervision of securities settlement transactions. The National Bank of Belgium has been designated to schedule and chair meetings of the authorities, as well as to organise certain information exchanges with the ESES CSDs. The Banque de France participates as the overseer of ESES France. However, each ESES supervisor/overseer remains responsible for performing its duties and exercising its powers vis-à-vis the national SSS/CSD, in particular in light of the powers CSDR grants competent authorities. The current arrangement has been maintained (with certain adaptations to take into account these regulatory powers), which enables the French, Belgian and Dutch authorities to closely coordinate their study of CSDR issues, reflecting the very similar operation and characteristics of the three ESES CSDs.

Formal assessments of the securities settlement system against international standards (PFMI) were performed regularly, generally every three years. The assessment process against these principles has been replaced by an assessment under the provisions of CSDR since CSDR came into force. The most recent assessment of the ESES CSDs, including Euroclear France, and their securities settlement system, was published in September 2015 on the Banque de France website. That assessment was the product of the joint work of six authorities, comprising the central banks and market authorities of each of the three countries in which the ESES CSDs are established. The assessment concluded that the ESES CSDs were in full compliance with the applicable principles, except three principles for which they were deemed broadly compliant: principle 19 on tiered participation arrangements, principle 20 on links between financial market infrastructures, and principle 23 on disclosure of rules, key procedures and market data.

Since the implementation of CSDR, the Banque de France is not only the oversight authority for ESES France's securities settlement system pursuant to the duties assigned to it by the *Code monétaire et financier*, but it is also the competent authority for Euroclear France. The AMF is also the competent authority for Euroclear France under CSDR, and it was already the supervisory authority for Euroclear France under French law.

Euroclear France is currently undergoing the CSDR authorisation process (see Section 1|4). For this purpose, it submitted an application in September 2017, which is being reviewed by the competent authorities.

The application of CSDR requires a certain number of changes for European CSDs in order to comply with the harmonised provisions adopted by this regulation. Most of these changes had already been introduced, or were in the process of being implemented following oversight assessments pursuant to the PFMI. For example, preparing an appropriate recovery plan is now a regulatory requirement applicable to CSDs and, therefore, the

recovery plan of the ESES CSDs, the first version of which dates from 2014, is fine-tuned annually.

2|3 CORE(FR)

Activity

CORE(FR), the French retail payment system, is operated by STET SA (*Systèmes Technologiques d'Échanges et de Traitement*). It allows its participants, which are French banks, to combine and submit domestic retail transactions. These transactions are then cleared daily and the net balance of each participant is calculated. Multilateral net positions are settled daily in TARGET2-Banque de France at 3.00 pm.

In 2017, 12.5 billion transactions, with a value somewhat exceeding EUR 4,800 billion, were cleared in CORE(FR). Between 2014 and end-2016, the volume of transactions cleared in CORE(FR) grew by 4.4% and increased in value by 3.1%. The volume of transactions in CORE(FR) fell at end-2016 due to the migration of clearing services for direct debits in the SEPA European format (SEPA direct debits) from CORE(FR) to the new SEPA.EU system, which was created in November 2016, and is also operated by STET (see Section 2|4). In 2017, between 949 million and 1,144 million transactions were settled monthly, representing values of between EUR 370 billion and EUR 452 billion. The progression of CORE(FR)'s activity, by volume and value, is shown in the Charts 5a and 5b.

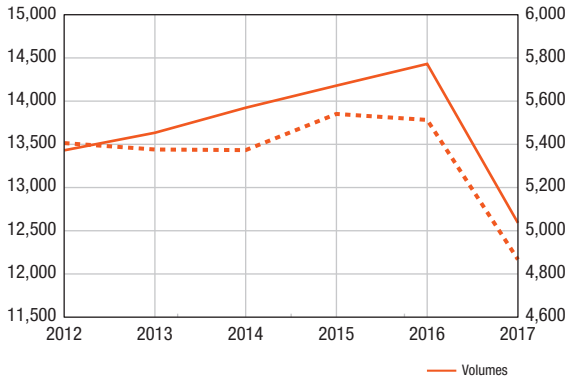
Due to the significant number of transactions it processes each day, CORE(FR) is covered by a financial protection mechanism. This financial protection mechanism takes the form of a mutual guarantee fund (EUR 800.5 million at end-2016, reduced to EUR 650.5 million in November 2017), which may be supplemented by individual guarantee calls to cover the highest net debt position.

Since late February 2013, STET has hosted the *Centre d'échange et compensation* (CEC – Centre for Exchange and Clearing) on the CORE platform for the Belgian community. It acts as a critical service provider for the system managed by CEC and overseen by the National Bank of Belgium.

C5 Activity in CORE(FR)

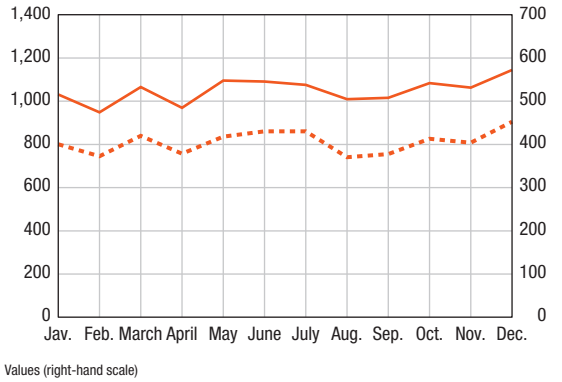
a) Since 2012

(volumes in millions of transactions, values in EUR billions)



b) In 2017

(volumes in millions of transactions, values in EUR billions)



Sources : STET, Banque de France.

Recent changes and development projects

On 21 November 2016, STET launched the operation of SEPA.EU, a pan-European clearing and settlement system for SEPA payments. SEPA direct debits (SDDs), which were previously processed in CORE(FR), are now processed and cleared in SEPA.EU (see Section 2|4). The Banque de France conducted a preliminary assessment of this major change to ensure that the future system would be in compliance with the principles applicable to it. The successful migration of these instruments from CORE(FR) to SEPA.EU was carried out inter alia through regular consultations with the client committee of CORE(FR), the system's governing body, as well as with technical committees, a harmonisation of the system's operating rules with the European Payments Council's (EPC) transposed credit transfer and direct debit rules, and an appropriate allocation of technical resources.

The Banque de France monitored these various activities and assessed whether the implementation thereof was in compliance with the supervisory framework, in order to maintain the security and effectiveness of CORE(FR) during and after this migration.

Assessment

On the basis of the classification criteria of ECB Regulation 795/2014 on oversight requirements for systemically important payment systems (SIPS), in August 2014, the ECB Governing Council designated CORE(FR) as a SIPS, together with the pan-European systems TARGET2, EURO1 and STEP2-T. In fact, CORE(FR) meets two of the four criteria established by the regulation, i.e. the daily value of payments processed by the system (more than EUR 10 billion) and its market share of the total volume of euro-denominated payments.[20]

On 13 August 2014, the ECB Governing council designated the Banque de France as the competent authority to oversee CORE(FR). Because the ECB oversees the other three pan-European systems referred to above, the Banque de France is currently the only Eurosystem national central bank with oversight authority over a SIPS.

In 2016, the Banque de France finalised its assessment report of CORE(FR), as required by ECB Regulation 795/2014, in conjunction with the Eurosystem's assessment of the other three systemically important payment systems. The system was deemed to be broadly compliant with the regulation. At the time the assessment was finalised on 31 January 2016, the operator planned to take various actions to bring the system into full compliance with all provisions of the regulation.

Since this assessment, STET, the operator, has implemented most of the actions requested, and the remaining actions are being closely monitored by the Banque de France, which receives frequent updates and regularly reports thereon to the Eurosystem.

In addition, the Banque de France made recommendations to the operator, most of which have also been implemented, which go beyond the requirements of the ECB Regulation and aim to further improve the system's risk management process.

2|4 SEPA.EU

Activity

SEPA.EU is the pan-European retail payment system operated by STET, which also operates CORE(FR). SEPA.EU, which began doing business on 21 November 2016, settles SEPA payment instruments, i.e. SEPA credit transfers (SCTs) and SEPA direct debits (SDDs). Initially, before its service was deployed at the European level, SEPA.EU served the community of French banks that were also CORE(FR) participants. Since it was

20 The four criteria are: the daily value of payments processed, market share, cross-border activity and services provided to other financial market infrastructures.

launched, the system processes and clears direct debits that were formerly processed in CORE(FR).

From 21 November to 30 December 2016, 235.65 million transactions (SDD direct debits), with a value of EUR 120.48 billion, were settled in SEPA.EU. In 2017, the volume of transactions settled was stable (between 196 and 229 million transactions per month), and the monthly values settled varied between approximately EUR 74 and EUR 106 billion (See Chart 6).

Recent changes and development projects

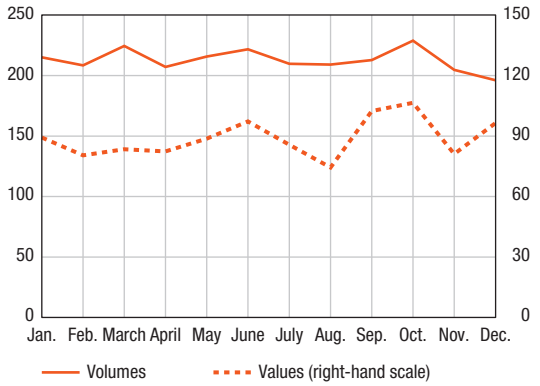
The following projects are ongoing.

• The migration of SCTs from CORE(FR) to SEPA.EU: STET will migrate credit transfers (SCTs) from CORE(FR) to SEPA.EU in March 2019. Unlike the current system used by CORE(FR), which operates on the basis of a single 24-hour cycle, in SEPA.EU the cycle concept will be replaced by continuous settlement with a prefunding model.

• The launch of an optional instant payment settlement service: CSM (Clearing and Settlement Mechanism) Instant Payment is an instant credit transfer settlement service that is based on the "SCT Inst" scheme developed by the EPC,[21] and that will be incorporated into SEPA.EU. This is a joint project of the French and Belgian banking communities, although they have different schedules for implementing the service. The official launch of the service on the market is planned for November 2018. The Banque de France will conduct a preliminary assessment of this initiative in order to determine if the changes CSM Instant Payment will generate within SEPA.EU may alter compliance with the nine principles for financial market infrastructure applicable to SEPA.EU (see below). Furthermore, operational risk management will be overseen jointly by the Banque de France and the National Bank of Belgium pursuant to a memorandum of understanding concluded by the two authorities.

C6 Activity in SEPA.EU in 2017

(volumes in millions of transactions, values in EUR billions)



Sources : STET, Banque de France.

Assessment

Although legally CORE(FR) and SEPA.EU are two separate systems, they nevertheless have common characteristics. Since it was launched, SEPA.EU operates on the same technical platform as CORE(FR) and has the same governance structure. However, because in the medium-term SEPA.EU will become a system independent from CORE(FR), for supervisory purposes, the Banque de France considers SEPA.EU to be a separate system, and in November 2016, gave notice thereof to the ESMA pursuant to the Settlement Finality Directive. Therefore, it is included in the list of payment and securities settlement systems designated under that directive and operating in France.

Pursuant to Article L141-4 of the *Code monétaire et financier*, the Banque de France is the competent authority responsible for oversight. Because, on an annual basis, SEPA.EU settles payment volumes representing less than 25% of the market for domestic payments, this system falls into the category of "Other Retail Payment Systems" (ORPS), according to the classification methodology of the Eurosystem.[22] This category of payment system is assessed on the basis of its compliance with

21 The EPC SCT Inst is a pan-European scheme for SEPA credit transfers developed by the European Payments Council, which aims to process transactions in real time, 24 hours a day, 7 days a week, 365 days a year.

22 *https://www.ecb.europa.eu/pub/pdf/other/Revised_oversight_framework_for_retail_payment_systems.pdf*

the nine CPMI-IOSCO Principles for Financial Market Infrastructures (PFMI).[23]

In July 2017, the Banque de France finalised its report assessing the compliance of SEPA.EU with the PFMI requirements applicable to ORPS. The system was deemed broadly compliant with the nine principles applicable to it. In September 2017, following this assessment, STET submitted an action plan to the Banque de France, in which it proposed corrective measures in response to the overseer's recommendations. Implementation of the remaining recommendations is closely monitored by the Banque de France, which regularly reports thereon to the Eurosystem.

2|5 Cooperative oversight

European central counterparties

The Banque de France is a member of the EMIR colleges of several European CCPs, pursuant to Article 18 of EMIR. During the period under review, it participated in the colleges of the Italian CCP Cassa di Compenzacione e Garanzia (CC&G), with which the French CCP has interoperability arrangements, the German CCP Eurex Clearing AG and the Dutch CCP EuroCCP, as the overseer of the central securities depository (Euroclear France) with which these CCPs have links. The Banque de France is also the alternate for the ECB, in its capacity as central bank of issue, on the EMIR college of the British CCP LCH Ltd.

TARGET2

Since 2008, TARGET2 has been the real time gross settlement (RTGS) system for the euro zone. The system was developed by three central banks: Banque de France, Deutsche Bundesbank and Banca d'Italia. In 2016, the system included 24 national central banks (and the ECB) and their national user communities. The participating central banks are the 19 euro zone central banks and the central banks of 5 other EU countries that are not members of the euro zone (Bulgaria, Croatia, Denmark, Poland and Romania).

Like the CORE(FR) French system, TARGET2 was identified as a SIPS by a decision of the Governing Council in August 2014 and, therefore, is subject to the requirements of ECB Regulation 795/2014 of 3 July 2014, as amended by ECB Regulation 2017/2094 of 3 November 2017. The ECB coordinates the oversight of TARGET2, with the cooperation of the national central banks that participate in the system.

The TARGET2 system was assessed in 2015 under the direction of the ECB, in conjunction with the central banks of the euro zone that volunteered to contribute to this assessment procedure.

At the time the assessment was finalised, on 31 January 2016, the operator planned to take various actions to bring the system into full compliance with all provisions of the regulation. Since this assessment, the TARGET2 operator has implemented most of the actions requested, and the remaining actions are being closely monitored by the ECB, which receives frequent updates thereon.

TARGET2-Securities

Although TARGET2-Securities (T2S) does not meet the definition of a securities settlement "system" within the meaning of the Settlement Finality Directive and therefore is not overseen as such, the Eurosystem nevertheless applies an oversight procedure similar to that applicable to securities settlement systems because the fact that it is a pan-European settlement platform makes it systemically important. The ECB is the lead overseer of T2S, with the active participation of all national central banks, which validate its approach and conclusions.

Furthermore, T2S is overseen jointly by the central banks and financial market authorities of the various jurisdictions in which at least one CSD

23 The relevant nine principles are legal basis (principle 1), governance (principle 2), framework for the comprehensive management of risks (principle 3), settlement finality (principle 8), participant-default rules and procedures (principle 13), operational risk (principle 17), access and participation requirements (principle 18), efficiency and effectiveness (principle 21) and disclosure of rules, key procedures and market data (principle 23).

has contractually outsourced its settlement service to T2S. This cooperative group oversight body is co-chaired by the ECB and ESMA. The 24 CSDs that migrated to T2S during the five initial migration waves are established in 21 Member States of the EU and the European Economic Area. Therefore, the supervisory group includes 21 central national banks and 21 national market authorities, in addition to ESMA and the ECB.

A preliminary assessment of T2S against the ESCB-CESR standards[24] was finalised in early 2014, and then published by the ECB and ESMA. The assessment against certain standards was not completed, in particular with respect to settlement finality, due to the fact that final common rules legally enforceable against third parties had not yet been adopted. Since then, as cash accounts are legally within the national systems comprising T2 (e.g. TARGET2-Banque de France), the "cash" component of T2S is included in the global assessment of TARGET2,[25] which is conducted against the PFMI.

Starting in early 2018, T2S will undergo a new and exhaustive oversight assessment, this time against the PFMI. Initially, the T2S operator will be required to furnish a self-assessment by completing a questionnaire. The final assessment will be based on this self-assessment, which will be critically analysed, inter alia by comparing it with all T2S documentation (contracts, operating manuals, etc.). Certain topics will be substantively assessed for the first time, in particular settlement finality in T2S, due to the signature of a memorandum of agreement by all CSDs and central banks participating in T2S, the concrete transposition of these principles into common procedures and the addition of new functionalities in T2S.

EURO1 and STEP2-T

Under the aegis of the ECB, as lead overseer, the Banque de France participates in the cooperative oversight of the pan-European payment systems operated by EBA Clearing: EURO1 (large-value payment system) and STEP2 (retail payment system processing SEPA credit transfers (SCTs) and SEPA direct debit (SDDs)).

The Banque de France has contributed to the various assessments conducted by the ECB, in particular with respect to these two systems' compliance with the Regulation on SIPS (see Section 1|3 above), as well as to monitoring action plans and the implementation of RT1, EBA Clearing's pan-European instant payment solution, which has been operational since 21 November 2017.

SWIFT

In connection with the cooperative oversight of SWIFT conducted by the National Bank of Belgium, in which the Banque de France participates, the oversight work during the period under review focused primarily on the Customer Security Programme, a programme for all SWIFT customers that aims to improve the cybersecurity of their local environments, the prevention and detection of attacks, and the reaction processes in the event of an incident:

- by taking part in the public consultation conducted by SWIFT;
- by granting agreement to SWIFT to continue the various aspects of its programme after having studied each fundamental principle and document;
- by entering into contact with the community of SWIFT users during the series of presentations about the Programme.

CLS

The CLS system provides payment versus payment (PvP) settlement of payment instructions for spot transactions in the foreign exchange market, certain listed currency derivatives and currency swaps. Each system participant holds a multi-currency

24 The ESCB-CESR standards were non-binding standards adopted by European regulators for the supervision of CSDs and SSS in particular. They were replaced by the PFMI in 2012.

25 The report assessing TARGET2 against the PFMI can be viewed at: *http://www.ecb.europa.eu/pub/pdf/other/t2disclosurereport201606.en.pdf?8341c2a74d87b322292738afa9c331a3*

account with CLS Bank International[26] with positions in each currency settled by the system. For its part, CLS Bank International holds accounts with the various central banks of issue of the relevant currencies. The CLS system began its settlement business in September 2002. By the end of 2015, it had 18 eligible currencies.

Due to its international scope involving numerous currencies, the CLS system is subject to cooperative oversight governed by an agreement (the "Protocol") between the Group of Ten (G10) central banks and the central banks whose currencies are settled by CLS. The Federal Reserve coordinates this oversight as lead overseer. The aim of this cooperation arrangement is to enable relevant central banks to participate in the oversight of the system and ensure its security and efficiency. Under this framework, the central banks verify CLS's compliance with the standards applicable to payment systems and financial market infrastructures, and study changes proposed by the operator, in order to assess potential impacts on the system's operating rules and conditions and, in particular, on its risk profile. The Oversight Committee, which is led by the Federal Reserve Bank of New York (FRBNY), and which comprises the signatory central banks, including the Banque de France, is the vehicle for this cooperation.

26 CLS's legal structure comprises CLS Group Holding AG, a Swiss holding company that represents the shareholders (the participating banks), and which holds CLS UK Intermediate Holding, an English company that provides various services to its subsidiaries, CLS Bank International and CLS Services Ltd. CLS Bank International is based in New York and holds participants' accounts, whereas CLS Services Ltd, which is based in London, provides operational services to CLS Bank International.

Oversight of cashless payment instruments between 2015 and 2017

1| Regulatory changes in the field of cashless payment instruments

1|1 The application of the second European payment services directive

Convergence of payments market regulations is an essential aspect of the integration of the payments market in Europe, which supplements major political initiatives such as the adoption of the euro as a currency or setting up SEPA (Single Euro Payments Area) payment instruments. The first European payment services directive and the two European electronic money directives, which were adopted in the 2000s, aimed to create a harmonised regulatory framework for payment services in Europe, while providing added consumer protection and encouraging competition in the market.

The second European payment services directive (PSD2), which was adopted on 25 November 2015 and entered into force on 13 January 2018, builds on these laws and expands the scope of regulated payment services to include new services and operators, and at the same time tightens the security requirements applicable to players in the payments market. After having participated in the negotiations that led to the adoption of the directive, the Banque de France was heavily involved in drafting the transposition order that was published in the *Journal officiel* on 10 August 2017.

The PSD2 creates a payment service provider (PSP) status for third parties that access accounts held by "account servicing" PSPs (primarily banks) to initiate payments or aggregate account information:

- payment initiators are intermediaries that are authorised to initiate payments, usually credit transfers, from a client's online bank account, and that offer these payment services to online merchants as a possible alternative to payment using a card or electronic wallet;

- information aggregators offer a service that consolidates information from various payment accounts a client may hold with other payment service providers.

These activities, which up to now had been conducted without regulatory supervision, carry a high risk of fraud as they require users to disclose to a third party the identifiers and access codes to their online accounts. In view of these new

circumstances, the regulation provides that bank identifiers may be shared with third-party PSPs if they are protected, in particular by encrypting data. It also provides that third-party PSPs and account servicing PSPs, as well as users, should communicate securely by using an interface, the characteristics of which will be specified in a level two regulation associated with the directive.

The directive also aims to enhance the security of payments on the basis of the following two principles:

- strong account holder authentication is required to access accounts and for all high-risk online actions (e.g. creating a new payee for credit transfers on an online banking site);

- strong payer authentication is required to initiate payments electronically.

However, exceptions to this obligation to use strong authentication may be defined in the regulations for transactions deemed low-risk (e.g. low-value payments or a credit transfer between accounts held by the same person).

The European Banking Authority (EBA) was tasked with preparing, in close collaboration with the European Central Bank (ECB), a regulatory technical standard setting out: (i) the requirements for, and exemptions from, strong customer authentication for securing transactions and access to accounts; (ii) the requirements for protecting personalised security credentials; and (iii) the technical and operational procedures enabling banks, third-party PSPs and their clients to communicate securely. To allow players to adapt their IT systems, the provisions of the directive covered by this technical standard will be applicable 18 months after the standard is adopted.

In addition to its contribution to this regulatory technical standard, the Banque de France also contributed to the preparation of two other documents that clarify the provisions of the directive in connection with its payment instruments oversight duties:

- the EBA guidelines on major incidents reporting, which was published on 27 July 2017;

- the EBA guidelines on operational risk and security, which was published on 12 December 2017.

These two guidelines entered into force at the same time as PSD2, i.e. 13 January 2018.

1|2 Instant payment: the European Payments Council's SCT Inst scheme

As electronic commerce has expanded, the need for faster execution of transactions has become a major issue in relation to the modernisation of payments, making "instant" payments a key topic in recent years. For this reason, in December 2014, the Euro Retail Payments Board (ERPB) initiated European work on this issue, which led it, firstly, to define instant payments as electronic payment solutions available 24 hours a day resulting in immediate interbank clearing and crediting of the payee's account and, secondly, to direct European industry players to develop a pan European solution as quickly as possible.

In November 2016, this work culminated in a presentation by the European Payments Council (EPC) of a pan-European instant payment project in accordance with the ERPB's definition. This solution should make it possible to make payments in euro in less than ten seconds 24/7, in the form of instant SEPA credit transfers (known as "SCT Inst"). Payment service providers that are EPC members have been able to offer this solution since November 2017 – the date the SCT Inst scheme adopted by the EPC took effect. However, enrolment in this scheme by banks is voluntary, and they are free to decide whether or not to offer instant credit transfer services to their clients.

To properly prepare the French market for the implementation of this pan-European payment

Box 3

Strong customer authentication

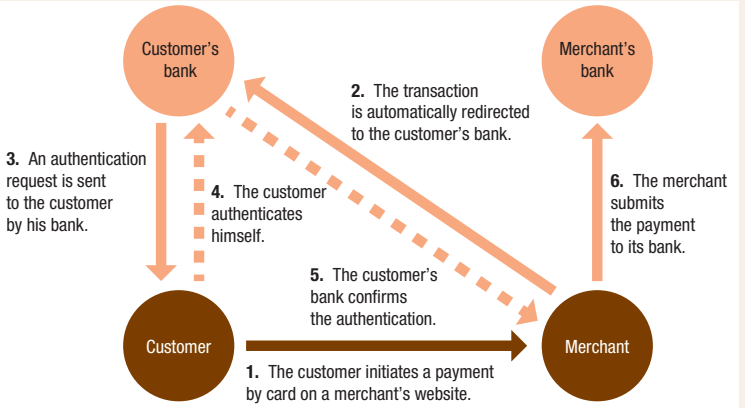
The issue of securing internet payments was raised in 2008 within the *Observatoire de la sécurité des cartes de paiement* (OSCP) at the instigation of the Banque de France. The recommendations the Observatory made in its 2009 annual report defined the concept of strong customer authentication, and invited French payment card market players to develop and implement authentication solutions meeting this definition.

The French example inspired the work conducted at the European level, firstly by the SecuRe Pay European forum, and then by the European Commission in preparation for the second European payment services directive (PSD2). The new directive defines strong authentication as a set of procedures based on the use of two or more of the following components:

- something only the user knows, e.g. a password or PIN;
- something only the user possesses, e.g. a token, mobile phone or smart card;
- something the user is, e.g. a biometric characteristic, such as a fingerprint or voice.

The elements selected must be mutually independent, i.e. the breach of one does not compromise the other(s). At least one of the components should be non-reusable and non-replicable (except for biometric characteristics). The strong authentication procedure should be designed to protect the confidentiality of authentication data.

Currently, strong authentication for payments is most frequently based on the use of a one-time password (OTP) given to the customer using a variety of channels, for example a text message to a mobile phone, a password generated on the customer's online banking website, or a card reader, display card or token.[1] When a payment is being made, the e-commerce website puts the customer in touch with the card-issuing bank so that it can authenticate the customer through the current protocol, 3D-Secure (see Diagram).



1 The 2015 annual report of the *Observatoire de la sécurité des cartes de paiement* provides a review of the strong authentication techniques most commonly used in France: *https://www.banque-france.fr/sites/default/files/medias/documents/oscp-rapport-annuel-2015.pdf*

solution, in 2016 the *Comité national des paiements scripturaux* (CNPS) identified the conditions for developing offers in relation to instant credit transfers, paying particular attention to the benefits and risks associated with the use thereof, and defined the various foreseeable circumstances in which the solution could be used.

Furthermore, to encourage rapid and secure adoption of this new payment method, since June 2017, the ECB and all Eurosystem central banks have been conducting a joint assessment of the SCT Inst scheme under the applicable oversight framework. The ECB will publish the results of this work in the spring of 2018.

Box 4

Support for the development of FinTechs in the payments field in France

FinTechs (a contraction of "finance" and "technology") are innovative businesses that develop value added services by applying the most advanced digital technologies (mobile and telecommunications technologies, biometrics, artificial intelligence, big data, blockchains, etc.) to the banking, finance and insurance fields.

In the payments field, FinTechs have a high growth potential. The French authorities have already taken specific measures to promote their development.

- Various types of regulatory status adapted to launching FinTechs: Law No. 2016-1321 for a Digital Republic, which was adopted and promulgated on 7 October 2016, amended the *Code monétaire et financier* by adding a provision that should facilitate the development of FinTechs while awaiting the transposition of the second European payment services directive (PSD2). Businesses that provide payment services that can be used exclusively within a limited network of acceptors or to purchase a limited range of goods or services, and whose business volume over 12 months is less than EUR 1 million, no longer are required to carry out any formalities with the *Autorité de contrôle prudentiel et de resolution* (ACPR). For several years, the French law has also granted payment institutions (PIs) and electronic money institutions (EMIs) authorisations under a relaxed prudential status, in particular with lower minimum capital and own funds requirements. Establishments may be authorised under these statuses if their volume of business is low (EUR 3 million in payments managed monthly in the case of PIs, a monthly average of EUR 5 million in electronic money in circulation in the case of EMIs). However, these relaxed statuses are not eligible for the European passport.

- Concerning the new account and payment initiation information aggregation services, before the entry into force of PSD2, the Banque de France, as well as the ACPR, met with FinTechs eligible for the new statuses created by the directive, in particular to provide assistance in preparing their authorisation applications. The primary aim of the Banque de France was to provide clarification on the security provisions relevant to these two new services.

- The oversight actions of the Banque de France cover the entire lifecycle of FinTechs, from the authorisation of payment and EMIs, in order to assess the security of payment services offered, to the annual collection of statistical data and regulatory information. These actions are guided by two additional principles: (i) a minimum set of security requirements, in particular in relation to sensitive payment data and authentication methods, and (ii) a proportionate approach to risks for the application of oversight requirements (with respect to governance, risk control, continuity, etc.).

1|3 Creation of the *Comité national des paiements scripturaux*

The *Comité national des paiements scripturaux* (CNPS – National Cashless Payments Committee), which succeeded the National SEPA Committee, was created in April 2016. It is chaired by the Banque de France, with the *Association française des trésoriers d'entreprise* (AFTE – French Corporate Treasurers Association) and the *Fédération bancaire française* (FBF – French Banking Federation) acting as vice-chairs. The purpose of this Committee is to offer a structure for dialogue for all French payment instruments stakeholders (representatives of users, service providers and the public authorities) that contributes to ensuring proper implementation of the national cashless payments strategy, which was launched in October 2015 by the Ministry for the Economy and Finance,[1] and the influence of the French community on upcoming changes in European payment systems.

1 *http://www.economie.gouv.fr/files/files/PDF/Strategienationale_sur_moyens_de_paiement_102015.pdf*

To achieve these objectives, the work of the Committee focuses on three priorities.

• Diversifying the payment offer of the public sector. The Committee offers a forum for consultation on the initiatives of players in the public and corporate sphere that aim to offer subscribers payment instruments better suited to their needs, as well as to those of the public sphere.

• The use by businesses of the new instruments in the SEPA range, in particular, "instant" credit transfers, which are the subject of a pan-European project coordinated by the ERPB. For example, the Committee has launched functional and technical projects to ensure proper implementation of the instant credit transfer in France. It has also focused on developing the accounting referencing functionalities for electronic payment orders, such as SEPA credit transfers, which numerous businesses have identified as an important prerequisite for the use of this payment instrument. The expansion of these payment instruments should lead to a decreased use of cheques, as they come to be seen as alternatives, in particular for business-to-business payments.

• The use of fast, secure and accessible electronic instruments by the general public, including for small amounts. To this end, and with the goal of enabling the general public to benefit from innovations in the payments field, the Committee monitors the commitments made to reduce pricing and technical obstacles to payment using cards for transactions with a value starting at one euro. A system has also been set up for monitoring the use of contactless payments, as well as for actively following innovations in the field of payments.

The actions conducted pursuant to these priorities all include a significant communication component, aimed at both businesses and the general public. Accordingly, two flyers, prepared in conjunction with the *Comité consultatif du secteur financier* (Financial Sector Advisory Committee), on, respectively, SEPA credit transfers and alternatives to payment by cheque, were published in May 2017. At the European level, these actions also included monitoring and contributing to the work on dematerialising the payment chain.

1|4 Creation of the *Observatoire de la sécurité des moyens de paiement*

The *Observatoire de la sécurité des cartes de paiement* (OSCP – Observatory for Payment Card Security) was created by the Law of 15 November 2001 on day-to-day security and established, at the national level, a consultation body tasked with enhancing the security of payment card transactions.

Bolstered by the diversity of its members, who are a representative cross-sample of all parties concerned by the security of payment cards, including service providers (banks, payment card systems), users (consumers, merchants and businesses) and the public authorities, throughout its existence the OSCP has made significant contributions to enhancing the security of payment cards in France, in particular by:

• collecting and publishing annually statistics on payment card fraud;

• enhancing the security of internet payments by promoting the use of strong cardholder authentication measures at the time of payment;

• enhancing the security of contactless payments by card or by mobile phone;

• enhancing the security of innovative mobile payment acceptance solutions.

The work of the OSCP has contributed to increasing the expertise of the Banque de France with respect to card security, enabling it to make proposals at the European level concerning regulatory requirements and applicable oversight frameworks.

Building on the successful work of the OSCP, and consistently with the national payments strategy launched in October 2015 by the Minister for the Economy and Finance, the Law of 9 December 2016 on transparency, preventing corruption and modernising the economy, expanded the remit of the OSCP to all cashless payment instruments.

The *Observatoire de la sécurité des moyens de paiement* (OSMP – Observatory for the Security of Payment Means) has taken over the duties of the OSCP – monitoring security enhancement measures undertaken by issuers, merchants and businesses, compiling statistics on fraud, and monitoring technological developments in relation to payment instruments – over a scope that has now been expanded to include cashless payment instruments. This broader scope will enable it to perform the security analyses that are indispensable for the work performed by the *Comité national des paiements scripturaux* (CNPS), which oversees implementation of the national payments strategy.

The members of the newly created OSMP were appointed on 20 June 2017 by an order of the Minister for Economy and Finance. Its membership continues to follow the principle of equal representation between service suppliers and users that had been followed by the OSCP. The Banque de France continues to act as chair (a position held by its Governor) and secretary for this new Observatory.

The initial work of the OSMP focused on harmonising the methods for collecting statistics about fraud concerning various payment instruments. Its first annual report, which was published on 18 July 2017 and is available on its website,[2] provides a statistical overview of fraud affecting cashless payments in France in 2016.

Its upcoming work will focus inter alia on the procedures for implementing enhanced authentication for payment instruments other than cards, as required by the PSD2.

2 *https://www.banque-france.fr/en/financial-stability/observatory-security-payment-means*

1|5 Updating of the cheque security framework

The cheque security framework (CSF), which was established for the first time in 2005 by the Banque de France, describes the security objectives that the Banque de France expects to be implemented by the institutions that participate in the various stages of cheque processing. It is supplemented by a cheque security assessment questionnaire, which breaks down the procedures for implementing these security objectives.

In late 2015, the Banque de France undertook the process of revising the CSF, in conjunction with the banking industry, through the *Comité français d'organisation et de normalisation bancaires* (CFONB – French Banking Organisation and Standardisation Committee). This project was deemed necessary due to a rapidly changing environment, driven by three initiatives.

- The definition of a national payment instruments strategy by the Ministry for the Economy and Finance, which encourages reducing the use of cheques in favour of electronic payment instruments.

- The need to encourage stakeholders to remain particularly vigilant with respect to managing risks associated with the use of cheques, and to adapt controls to better take into account the weak points of the cheque payment chain. In fact, cheques account for the second highest incidence of fraud involving payment instruments, behind cards, despite the fact that they are only the fourth most used payment instrument (behind cards, credit transfers and direct debits).

- The desire to adapt the CSF to the format used by the security frameworks for other cashless payment instruments established by the Eurosystem and the Banque de France.

This project culminated in a revised framework that defines nine security objectives applicable to cheque payment systems, i.e. all processes in connection with cheque-handling by institutions (See Box 5).

Box 5

The nine security objectives of the new cheque security framework

1. Governance and organisation

[…] Security governance aims to ensure that security measures are in place, and that they are optimal and appropriate. The stakeholders [who are participants in the cheque payment system] must have a set of formal, regularly updated documents that define this governance framework and the organisation of the security of the cheque payment system, covering all associated activities, including outsourced activities.

2. Risk assessment

Security management requires identifying assets to be protected associated with an analysis of risks incurred, as well as setting up organisational, technical and procedural measures that offer such protection. Measures deployed must be assessed periodically to determine their effectiveness.

3. Controlling and limiting risks

Stakeholders must implement adequate security measures in order to limit the risks identified, in accordance with the security policy of the business line.

4. Managing incidents and reports

Stakeholders must set up a system for monitoring incidents in connection with transactions and customer complaints that provides an exhaustive record of incidents. This monitoring system should include a procedure for reporting incidents that adequately informs the governance bodies, as well as relevant external parties.

5. Traceability - audit trail

Stakeholders must set up a process that provides traceability that can be used to create an uninterrupted audit trail for each transaction covered by the cheque payment system.

6. Physical security of cheques

Stakeholders must ensure the security of the physical media containing cheques throughout their lifecycle.

7. Security of operating environments

The physical and logical environments of the cheque payment system must be secure and protect the physical and logical media containing cheques, as well as the transactions carried out. They must ensure the quality, availability and technical usability of elements archived.

8. Transaction monitoring system

Transactions must be monitored to prevent, detect and block attempted payments suspected to be fraudulent. This oversight must be carried out pursuant to a formal procedure that defines the rules governing alerts, as well as the possible types of alerts.

9. Raising awareness among clients about security rules

Establishments must raise awareness among their clients about the precautionary rules for safeguarding pre-printed cheques, issuing and receiving cheques, keeping cheques and depositing cheques.

This new framework takes the form of a self-assessment questionnaire for banks, which has also been revised, and which is used to assess the level of compliance with each objective on the basis of a detailed analysis. Lastly, two annexes, one that describes the cheque payment system and the other that provides a concordance table cross-referencing the previous version of the framework, complete the new framework.

At the conclusion of a public consultation procedure with stakeholders during the summer of 2016, the Banque de France published the new framework on its website in the second half of that year.[3] The new framework took effect on 1 January 2017 for purposes of a first annual report by the various institutions, which is due in the first half of 2018.

3 *https://www.banque-france.fr/en/financial-stability/market-infrastructure-and-payment-systems/oversight-tasks/oversight-cashless-means-payment*

1|6 Changes in anonymous prepaid cards

Anonymous prepaid cards are an exception in the field of cashless payment instruments because they allow users to remain anonymous during transactions. Therefore, they can be used in money laundering and terrorism financing channels.

Box 6

Legal classification of prepaid cards and due diligence obligations of issuers

The French law defines electronic money in Article L315-1 of the *Code monétaire et financier* as "a monetary value stored in an electronic form, including a magnetic form, representing a claim against the issuer, which is issued against the delivery of funds for purposes of payment transactions […] and that is accepted by an individual or legal entity other than the issuer of the electronic money". Concretely, electronic money is most often usable in the form of "prepaid" cards that can be used to make purchases in a single payment circuit or in the same manner as any other payment card. These prepaid cards are most often backed by international card payment systems, such as Visa and MasterCard.

Electronic money institutions, like credit institutions, are subject to anti-money laundering and counter-financing of terrorism regulations, in particular the obligations to identify and verify the identity of the client, as well as know-your-customer obligations. However, Article R561-16 (5) of the *Code monétaire et financier* provides an exception to these obligations, subject to the following conditions:

- the electronic money is used only to purchase goods and services;
- the maximum amount of the medium cannot exceed EUR 250;
- if the medium can be reloaded, payments are limited to EUR 250 per 30-day period and can be used only within France;
- the medium cannot be loaded using electronic money that is itself anonymous or cash (except if the electronic money can be used only within a restricted acceptance circuit or for a restricted range of goods or services, such as is the case with gift cards).

These exceptions to the due diligence obligations, which had already been limited by the Decree of 10 November 2016 on combating the financing of terrorism that was adopted following the terrorist attacks in Paris, may be further restricted in connection with the transposition of the future fifth European anti-money laundering directive.

In addition, each cash reimbursement or cash withdrawal transaction for an amount over EUR 100 is subject to the above due diligence obligations.

Electronic money issued pursuant to this exception is known as anonymous electronic money. Therefore, for example, a non-reloadable prepaid electronic money card can be purchased (usually over the internet or from a local merchant) without the issuer being required to comply with the obligations to identify and verify the identity of the client if the preloaded amount does not exceed EUR 250.

Prepaid cards are regulated pursuant to the transposition of the second Electronic Money Directive (EMD2) by Law No. 2013-100 of 28 January 2013. The law provides that prepaid cards may be issued and managed only by electronic money issuers, i.e. institutions that have been authorised as electronic money institutions or credit institutions by the competent national authority of the issuer's country (in France, the *Autorité de contrôle prudentiel et de resolution* – ACPR) or by issuers authorised in the European Economic Area that hold a European passport.

Electronic money institutions and credit institutions are subject to the anti-money laundering and counter-financing of terrorism (AML-CFT) obligations of the Member State in which they are established, under the supervision of the competent authority of that Member State.

In response to the money laundering and financing of terrorism risks that these payment instruments create, the Banque de France, along with other relevant authorities, including the ACPR, which is responsible for supervising compliance with AML-CFT obligations by financial institutions established in France, and the French public authorities, has contributed to tightening the applicable requirements:

- at the European level, by proposing amendments to the fourth anti-money laundering and counter-financing of terrorism directive that would reduce the maximum anonymous electronic money threshold to EUR 150 (versus EUR 250 in the initial draft of the directive), limit cash reimbursements without verifying the holder's identity to EUR 50 (versus EUR 100), and requiring identification of the holder for internet payments;

- at the national level, by adopting restrictive measures on the issuance and use of prepaid cards (anonymous or otherwise), in particular limiting the maximum monetary value stored to EUR 10,000, limiting the maximum cash or electronic money reloading capacity to EUR 1,000 per month, and limiting cash withdrawal or reimbursement transactions to EUR 1,000 per month.

2 | Report on oversight of cashless payment instruments

2.1 Report on post-SEPA migration

In accordance with Regulation (EU) 260/2012, which provided additional time for "niche" products, the second phase of the migration to SEPA payment instruments was completed in France in February 2016. As a result, the interbank payment order (*titre interbancaire de paiement*) was replaced by the SEPA Core Direct Debit, and automatic electronic payment was replaced by the SEPA Core or Business-to-Business Direct Debit depending on the type of payer.

As secretary of the SEPA National Committee, and of the CNPS as of 2016, the Banque de France monitored this migration and observed the specific constraints associated with the use of the SEPA Business-to-Business Direct Debit. More specifically, the Banque de France analysed the requirement that the payer inform its bank before the first transaction that a direct debit mandate has been signed. These operational constraints created difficulties for creditors that chose this payment instrument, in particular public and social contribution payees, many of which experienced high rejection rates.

For this reason, in 2017, many creditors opted to replace the SEPA Business-to-Business Direct Debit with the SEPA Core Direct Debit. This new migration, which was coordinated by the CNPS, was successfully carried out in the summer of 2017. It has facilitated the direct debit payment process and improved the overall efficiency of payments for relevant users.[4]

4 Additional information on this topic can be found in the CNPS's first activity report, which is available at the following address: *https://www.banque-france.fr/sites/default/files/media/2017/07/18/cnps_2017_web.pdf*

2|2 Contribution of the Banque de France to the authorisation procedure for payment and electronic money institutions

In connection with its review of authorisation applications, the ACPR consults the Banque de France, in accordance with Article L141-4 of the *Code monétaire et financier*, on the technical, IT and organisational resources in relation to payment instrument security for the activities planned by the companies requesting authorisation. The Banque de France prepares an opinion in response to these consultations.

Between 1 January 2015 and 31 December 2017, the Banque de France prepared and provided 46 positive opinions to the ACPR on:

- 11 payment institution authorisation procedures;
- 3 electronic money institution authorisation procedures;
- 24 payment institution exemption procedures;
- 1 electronic money institution exemption procedure;
- 1 payment and electronic money institution dual exemption procedure;
- 3 extension procedures for the provision of other payment services of payment institutions;
- 3 extension procedures for the provision of other payment services of electronic money institutions.

These institutions are subject to Banque de France oversight, as are all payment service providers in France.[5] More specifically, they are subject to all obligations to submit reports to the Banque de France on annual fraud statistics, as well as describing changes to their risk management systems applicable to the payment services they provide. In addition, they are subject to onsite inspections.

2|3 Contribution to the Eurosystem's payment card oversight actions

In February 2015, the ECB published an updated version of the guide for the assessment of card payment systems,[6] which incorporates the recommendations made by the European Forum on the Security of Retail Payments on 31 January 2013 on the security of internet payments, which cover the following aspects of the security of internet payments:

- general control and security environment (governance, risk assessment and mitigation systems, monitoring and reporting incidents, traceability);
- specific control and security measures for internet payments (use of strong customer authentication, monitoring transactions, sensitive data protection, setting limits, providing transaction information to clients);
- educating clients and communications between clients and payment card issuers.

These recommendations tightened the requirements applicable to card payment systems, which prompted a fresh compliance assessment of all systems operating in Europe.

The first assessment of card payment systems had been completed in 2014, which was only one year before the new assessment guide took effect. Therefore, the Eurosystem decided to limit the second assessment to new requirements and requirements that had been amended. For this purpose, the national central banks of the European System of Central Banks were requested to individually assess each system operating in their respective countries, and to assist the central banks tasked with coordinating the assessment of international systems.[7] In addition to the assessment of the six French card payment systems[8] – the highest number in Europe – the Banque de France is one of the few central banks to have participated in the assessment of the

5 See *2014 Oversight Report* – Section 4.1.2. *https://www.banque-france.fr/sites/default/files/medias/documents/rapport-surveillance-moyens-paiement-et-infrastructures-marches-financiers_2014_en.pdf*

6 *http://www.ecb.europa.eu/pub/pdf/other/guideassessmentcpsagainstoversightstandards201502.en.pdf*

7 The European Central Bank for the American Express and Visa payment systems, and the National Bank of Belgium for MasterCard.

8 The Cartes Bancaires interbank payment system, as well as the five private payment systems of BNP Paribas Personal Finance, Cofidis, Crédit Agricole Consumer Finance, Franfinance and Oney Bank.

Box 7

Key security measures introduced by the European Central Bank recommendations in the assessment guide

Standard 3.1 – Security management

- Analysis of the security risks and policy of the card payment system to ensure they are consistent and updated regularly
- Ongoing monitoring of technological and security developments for the purposes of updating the risk profile
- Procedure for reporting, classifying and monitoring incidents
- Formal change management process
- Restrictive physical and logical access to infrastructures management policy
- Protection of sensitive data exchanged during transactions, based on advanced encryption techniques
- Continuity plan in the event sensitive data is compromised

Standard 3.2 – Manufacture and distribution of cards

- Minimum security requirements applicable to payment cards and terminals
- Secure procedures for communicating sensitive authentication information (PIN, telephone number for sending one-time passwords, etc.)
- Enrolment of cardholders in a strong authentication system for internet payments

Standard 3.3 – Transactions

- Limited validity of cards and authentication data
- Specific security specifications for the various types of card use, depending on the level of risk
- Mechanism for detecting unauthorised or fraudulent transactions
- Measures for limiting fraud (payment maximums per channel, mechanism for blocking cards, etc.)
- Mechanisms to encourage card payment system participants to use fraud reduction measures (e.g. transferring liability to the issuer if strong authentication used)

three international systems that underwent this process.

The assessments of the six French card payment systems showed a high level of compliance with oversight requirements, which had been facilitated by the actions that had been carried out since 2009 by the OSCP to reinforce the security of internet payments, which anticipated the requirements subsequently adopted by the European authorities.

2|4 Verification of the security and proper functioning of cheques and online payments

Pursuant to its duty to oversee cashless payment instruments, in accordance with Article L141-4 of the *Code monétaire et financier*, the Banque de France may carry out any expert assessment of payment instruments or the technical resources associated therewith that it deems necessary.

For this purpose, on-site inspections, conducted by the General Inspection function of the Banque de France, are regularly carried out. Two sets of on-site inspections were carried out between 2014 and 2016 within various French banking groups.

Inspections of the security and proper functioning of the cheque payment system

The aim of this set of inspections, which was conducted in the fourth quarter of 2014, was to assess the security and proper functioning of the management of cheque-related activities within various French banking groups and institutions that had been selected due to their size or because they were deemed representative. The matters reviewed in connection with these inspections included the organisation of the cheque use circuit (cheque production, distribution, deposits and processing) and detecting and monitoring fraud involving this payment instrument.

Cheque-related processes, which are frequently outsourced, appeared to be generally well supervised, and service providers were monitored satisfactorily by the institutions. Overall, the institutions were aware of the need for cheque fraud prevention measures, and had internal structures and tools in place dedicated to detecting and analysing such fraud. Nevertheless, several areas for improvement were suggested, in particular reinforcing internal control systems and enhancing the quality of fraud statistics reported to the Banque de France.

The information obtained from this set of inspections was also used in connection with the redrafting of the cheque security framework (see Section 1|5).

Inspections of compliance with the European Banking Authority's guidance on the security of internet payments

The aim of this second set of inspections, which was conducted in June and July 2016, was to ensure that internet payments administration and management processes were in compliance with the guidelines of the European Banking Authority (EBA), which took effect on 1 August 2015. These guidelines cover two main topics: the general control and security environment and specific control and security measures for internet payments. This set of inspections was focused on institutions with varying profiles, in terms of size, type of clients and services offered.

These inspections concluded that compliance with the EBA guidelines on the security of internet payment was satisfactory overall. The institutions were aware of fraud issues and took action to reinforce the security of their existing systems. Nevertheless, due to the fact that the range of sensitive payment data is expanding and is no longer limited to banking identifiers (card number, IBAN), particular care must be taken to protect other data, such as telephone numbers and e-mail addresses, which are now used for payment security operations and which therefore must be protected from phishing attacks.

The inspections also showed the progress made to secure transactions: strong customer authentication solutions have been deployed by all institutions inspected to secure access to internet payment initiation and to access sensitive payment data.

2|5 Report on oversight of special paperless payment orders

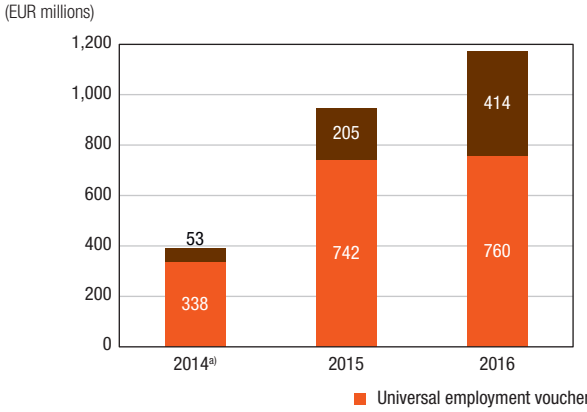
Pursuant to the duty to oversee the security of special paperless payment orders and universal employment vouchers assigned to it by Law No. 2013-100 of 28 January 2013, in 2014 the Banque de France set up an annual oversight procedure of issuers of these instruments, based on the collection of self-assessment questionnaires of issuers on their compliance with applicable security objectives, as well as the collection of operational and fraud statistics.[9]

The assessment of the first three years of oversight of special paperless payment orders and universal employment vouchers, covering the period from 2014 to 2016, shows the following.

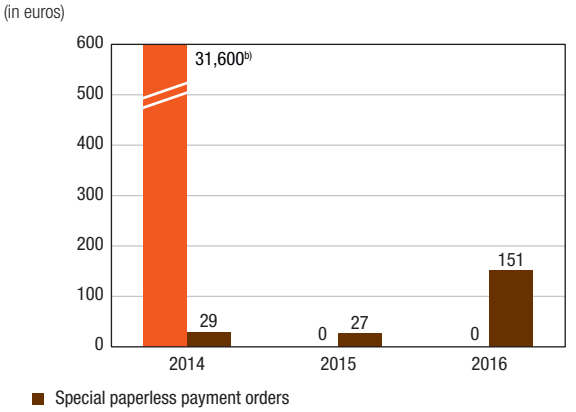
9 See *2014 Oversight Report*: https://www.banque-france.fr/sites/default/files/medias/documents/rapport-surveillance-moyens-paiement-et-infrastructures-marches-financiers_2014_en.pdf

G7 Use of universal employment vouchers and special paperless payment orders

a) Amount of payments



b) Amount of fraud



Universal employment vouchers Special paperless payment orders

Source: Banque de France.
a) Partial figures.
b) Exceptional case of internal fraud involving universal employment vouchers in a social welfare agency.

• In terms of volumes issued and used, these instruments account for a marginal share (0.004%) of all transactions involving cashless payment instruments, i.e. about EUR 1.2 billion in annual payments involving these instruments compared to EUR 499 billion in card payments and EUR 1,077 billion in cheque payments in 2016 (See Chart 7a).

Restrictive use conditions apply to these instruments, which make them less attractive as vehicles for fraud. In 2016, total fraud detected amounted to EUR 151, compared to EUR 27 in 2015 and EUR 31,629 in 2014 (due to an exceptional case of internal fraud involving universal employment vouchers in a social welfare agency). Therefore, the rate of fraud involving these instruments is very low compared to the rates for other payment instruments. For example, the rate of fraud involving special paperless payment orders is ten times lower than that for credit transfers, which, proportionally, is the payment instrument with the lowest rate of fraud (See Chart 7b).[10]

• Concerning issuers' compliance with the security objectives of the framework, the information furnished by issuers showed that special paperless payment orders and universal employment vouchers were globally compliant with all security objectives.

Based on these results, and in order to conduct oversight that is proportionate to the level of actual risk to which these instruments are exposed, the information collection procedures were relaxed as from 2017, in accordance with the following guidance.

• The frequency for collecting security objectives self-assessments was reduced: due to the satisfactory level of maturity observed with respect to the security objectives and the very low levels of fraud involving these two types of instruments, the self-assessment will now cover a three-year period. As a result, only new issuers will be requested to provide a self-assessment in years other than those in which self-assessments are collected.

• More frequent monitoring of fraud progression statistics, enabling prompt reaction in case of a deterioration in the level of security: therefore, data on the numbers of transactions, cases of fraud and attempted fraud, and the corresponding amounts will be collected quarterly rather than annually.

10 See the 2016 Annual Report of the *Observatoire de la sécurité des moyens de paiement*. *https://www.banque-france.fr/en/financial-stability/observatory-security-payment-means*

• Statistical data on other activities in relation to the issue of instruments will continue to be collected annually: continuing this annual data collection, in particular on the number of financiers and payees, as well as the volumes and amounts of instruments issued during the year and in circulation at year-end, is necessary to properly oversee developments in the issuance of these instruments (in particular, the migration of special paperless payment orders away from paper instruments).

Lastly, if the statistics collected quarterly were to show a significant increase in fraud, the Banque de France would initially activate its ongoing oversight system in order to take quick action vis-à-vis the relevant issuer (bilateral exchanges, recommendations), while reserving the right to reactivate the collection of data on security objectives if this is not an isolated event. Bilateral meetings would be held to discuss the results of such data collection

2|6 Oversight of complementary community currencies

Complementary community currencies, which are issued at the local level to encourage economic exchanges between local stakeholders, come within the category of "complementary community currency instruments" within the meaning of the *Code monétaire et financier*. The Code provides that such instruments are issued by undertakings pursuing community goals, as defined by the Law of 31 July 2014, and whose sole corporate purpose is to issue such instruments.

To engage in their activity, undertakings issuing or managing complementary community currency instruments are required to have payment service provider status. The actual authorisation arrangements depend on the approach taken to issuance, with exemption options available in each case.

Since these currency instruments are considered to be payment instruments, the Banque de France is in charge of overseeing their security if they are issued in cashless form. It also issues opinions on the security of these activities when reviewing authorisation and exemption applications filed with the ACPR.

2|7 Analysis of the risks associated with the development of crypto-assets

Cryptographic assets, such as bitcoin, ether or ripple, are not considered to be alternative currencies. They do not satisfy the three functions of money (unit of account, means of exchange and store of value), and also fail to meet the French Monetary and Financial Code's definition of means of payment and electronic money.

The Banque de France publicly warned, in particular in a Focus published on 5 March 2018[11], of the risks associated with crypto-assets, against the backdrop of the sharp increase in the total capitalisation of these assets, and is actively contributing to the discussions of the national, European and international authorities on avenues for their regulation.

The risks associated with the speculative nature of crypto-assets

The convertibility of crypto-assets into different fiat currencies is not guaranteed by any centralised authority. Therefore, investors can only recover their funds in other currencies if other users wish to acquire the same crypto-assets. Consequently, the price of a crypto-asset may at any time collapse if investors wishing to unwind their positions cannot find purchasers and become holders of illiquid portfolios.

In the particular case of bitcoin, the process of issuing units, which is solely dependent on hashing power, is capped over time. This limitation maintains their scarcity which, given the high demand, mainly for speculative purposes, results in very large price fluctuations.

11 *https://publications.banque-france.fr/sites/default/files/medias/documents/focus-16_2018_03_05_en.pdf*

Box 8

Avenues for regulation explored by public authorities

It is advisable to regulate activities associated with crypto-assets for four main reasons: anti-money laundering (AML) and combating the financing of terrorism (CFT) – which is a key priority – investor protection, preserving market integrity, including in the face of cyber-risks, and lastly, in the event of further growth in these activities, financial stability concerns.

The Banque de France and the *Autorité de contrôle prudentiel et de résolution* (ACPR) are advocating extending the regulation of the provision of services associated with crypto-assets in order to cover two areas

1. Regulating the services offered at the interface between the real economy and crypto-assets

The conversion of crypto-assets into fiat currency by internet platforms that play the role of intermediary between buyers and sellers is considered to be a payment service and requires an authorisation to provide such services. However, this requirement arises from the third-party management of accounts held and denominated in a fiat currency, and not from the provision of services associated with crypto-assets.

In addition to this approach, the Banque de France and the ACPR are advocating broadening the regulation of the provision of such services, by creating a crypto-asset services provider status.

These regulatory changes could stem from the revision of the Fifth Anti-Money Laundering Directive currently being adopted by the EU (known as 5MLD). This Directive provides for the regulation of players offering (i) the exchange of crypto-assets for fiat currencies and (ii) the storage, on behalf of private clients, of cryptographic keys that can hold, store or transfer crypto-assets.

The crypto-asset services provider status would make it possible, beyond the fight against money laundering and terrorist financing which is a priority, to subject market actors to rules governing operational security and customer protection This status could also cover services concerning transactions between crypto-assets This status could also cover services concerning transactions between crypto-assets.

2. Regulating investments in crypto-assets

The regulation of crypto-asset service providers could be supplemented by a limitation of the possibility for certain regulated companies (banks, insurers, asset management firms, etc.) to trade in crypto-assets. The first objective would be to ban deposits and loans in crypto-assets. As regards savings products, the marketing of any such investment vehicles to the general public should be considered, thus reserving these products for the most sophisticated investors. Furthermore, these products should be subject to stringent customer protection rules. Lastly, for the proprietary investments of regulated entities, the stringent regulation of these products, for example by deducting their total value from capital, should be considered. In order to implement these regulatory changes, national and European legislation would need to evolve.

For its part, the *Autorité des marchés financiers* (AMF) considers that the marketing of crypto-asset derivatives requires an authorisation and cannot be advertised electronically. In addition, following on from its public consultation on ICOs, the AMF has decided to continue its work on defining a regulatory framework specific to ICOs offering appropriate guarantees, notably regarding disclosure, which would be necessary for this new type of product offering. This work will be carried out in coordination with the other public authorities concerned.

Regulation should be coordinated at the European and international levels in order to ensure that it is more effective.

Since crypto-assets are dematerialised and use internet-based technologies, which promotes the provision of cross-border services, the patchwork nature of domestic regulations makes it impossible to fully manage the relevant risks.

It therefore appears necessary to discuss the regulation of crypto-assets at the international level. On 7 February 2018, the French and German Ministers of the Economy and Finance and central bankers requested the involvement of the G20 in this respect.

A diversification of uses that is exposing investors to increasing risk of losses

There is a growing interest in crypto-assets from outside their initial communities, i.e. from users and merchants not playing an operational role in the issuance and management of these assets (e.g. those not mining[12] crypto-assets). This is leading to the development of numerous services whose structure is based on that of existing services in the traditional financial sphere.

For instance, in the area of market infrastructures, exchange platforms on which crypto-assets can be bought and sold for fiat currencies (EUR, USD, etc.) have been created. These platforms enable users that have not participated in the creation process to acquire such assets, or convert into fiat currency crypto-assets received as payment. They have also spurred numerous services related to the storage of crypto-assets, which are similar to depositary activities.

In addition, they have fostered the development of services in the areas of financial disclosure and data provision, as well as investment advice and trading. These activities promote the creation of investment instruments backed by crypto-assets, such as funds or derivative instruments, similar to the initiatives of the Chicago Board Options Exchange or the Chicago Mercantile Exchange.

Financing activities have also benefited from the development of crypto-assets, through Initial Coin Offerings (ICOs). ICOs replicate the concept of crowdfunding but use crypto-assets instead: in this type of scheme, internet users funding projects (in crypto-assets or fiat money) receive in return digital assets (or tokens). In practice, these tokens represent an economic stake in the project. They offer their holders certain rights, such as priority access to the platform or financed application (like traditional crowdfunding), receiving a share in the firm's profits or voting rights (like shares). Since the management of tokens issued in ICOs is itself performed by the blockchain used for the ICOs, it is based on almost identical exchange mechanisms to those used by the crypto-assets. They therefore constitute an additional form of crypto-asset, carrying specific rights (privileged access to the financed project, voting rights, etc.). The limitations and the risks of the crypto-assets discussed here therefore also apply to these tokens.

Anonymous mechanisms that promote the financing of terrorism and criminal activities as well as the circumvention of anti-money laundering regulations

The anonymity surrounding the issuance and transfer of most crypto-assets makes it more likely for these assets to be used for criminal purposes (internet sales of illegal goods or services) or for money laundering or terrorist financing.

In France, the organisation Tracfin (responsible for Processing of Information and Action against Clandestine Financial Activities) has identified the use of crypto-assets, especially bitcoin, as posing a specific risk in the area of money laundering and terrorist financing.

Major cyber-risks for crypto-asset holders

The digital wallets that store these crypto-assets are known to be at risk of hacking. Against this backdrop, holders have no recourse in the event of their assets being stolen by hackers. Repeated incidents of major fraud (hacking of Coincheck in January 2018 where USD 534 million were stolen, or the momentous collapse in 2015 of MtGox, the first global bitcoin exchange[13]) illustrate the vulnerability of the crypto-asset ecosystem and the attendant high level of risk, in the absence of guarantee mechanisms.

An environmental cost inherent to the functioning of crypto-assets

The electronic validation of crypto-asset transactions also carries a considerable environmental cost arising from the energy resources involved: in December 2017, it was estimated that a single bitcoin transaction requires 215 kilowatt-hours of electricity to process. This energy consumption is constantly being revised upwards, due to the heightened competition stemming from the growing validation network.

12 Direct participants in the crypyo-asset issuance and management network who validate and register transactions via an algorithm in a "distributed" ledger are known as "miners".

13 Following an insider fraud leading to the disappearance of 650,000 bitcoins worth around USD 360 million.

CCP	Central counterparty
CLS	Continuous Link Settlement
CORE(FR)	French retail payment system
CPMI	Committee on Payments and Market Infrastructures
CPSS	Committee on Payment and Settlement Systems, which has been renamed CPMI
CSD	Central securities depositories
CSDR	Central Securities Depositories Regulation
EBA	European Banking Authority
EMIR	European Market Infrastructure Regulation
EPC	European Payments Council
ESCB-CESR	European System of Central Banks and Committee of European Securities Regulators
ESES France	Euroclear Settlement of Euronext-zone Securities France
ESMA	European Securities and Markets Authority
EURO1	Large value payment system
FSB	Financial Stability Board
IOSCO	International Organisation of Securities Commissions
LCH SA	French central counterparty
PFMI	Principles for Financial Market Infrastructures
SCT	SEPA Credit Transfer
SDD	SEPA Direct Debit
SEPA	Single Euro Payments Area
SEPA.EU	Pan-European retail payment system
SIPS	Systemically important payment systems

SSS	Securities settlement system
STEP2-T	Retail payment system
STET	*Systèmes Technologiques d'Échange et de Traitement*, operating CORE(FR)
SWIFT	Society for Worldwide Interbank Financial Telecommunication
T2S	TARGET2-Securities
TARGET2	Trans-European Automated Real-time Gross Settlement Express Transfer

For further information, see the Bank for International Settlements (BIS) glossary: *http://www.bis.org/cpmi/publ/d00b.htm*

Published by
Banque de France
39, rue Croix des Petits-Champs – 75001 Paris

Publishing Director
Nathalie Aufauvre
Director General of Financial Stability
and Operations
Banque de France

Executive Editor
Emmanuelle Assouan
Director of Payment Systems
and Market Infrastructures
Banque de France

Editorial Committee
Valérie Fasquelle, Deputy Director of Payment Systems and Market Infrastructures
Alexandra Andorra, Véronique Bugaj, Paul Capocci, Christelle Guiheneuc, Julien Lasalle, Antoine Lhuissier, Lucas Nozahic, Alexandre Stervinou, Mathieu Vileyn (SMPS), Samira Bourahla, Carole Fromont, Thomas Guérin, Claudine Hurman, Laurent Kersenbaume, Soraya Levy-Rueff, Claire Orliac, Clément Rouveyrol, Raphaël di Ruggiero, Arnaud Stien et Clay Youale (SEPI), Yann Testard, Audrey Metzger (SETIM), Nelly Noulin (SEL)

Technical production
Studio Création
Direction de la Communication

Printed by
Banque de France – SG - DISG

Registration of copyright
April 2018

Internet
https://publications.banque-france.fr/en