OVERSIGHT OF CASHLESS MEANS OF PAYMENT AND FINANCIAL MARKET INFRASTRUCTURES

REPORT 2020

OVERSIGHT OF CASHLESS MEANS OF PAYMENT AND FINANCIAL MARKET INFRASTRUCTURES

2020

TABLE OF CONTENTS

FOREWORD

Pursuant to Article L. 141-1 (I) and (II) of the *Code monétaire et financier* (Monetary and Financial Code), the Banque de France oversees:

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

Smooth functioning and security of financial market infrastructures and means of payment is vital for the entire economy. It enables monetary policy to be implemented effectively and contributes 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 means of payment. The last report was published in 2017.

This report covers the period from 2018 to 2020.

INTRODUCTION

Over the last three years, the oversight of market infrastructures and cashless means of payment, while maintaining continuity from the previous period, has seen several significant developments, which reflect amendments to the regulatory framework, as well as the emergence of new issues and the expansion of previously observed trends.

The regulatory framework, which had been extensively overhauled in previous years by the entry into force of several particularly significant regulations, such as the European Market Infrastructure Regulation (EMIR) on central counterparties (CCPs), the Central Securities Depositories Regulation (CSDR) and the second Payment Services Directive (PSD2), has been clarified by various technical standards and supplemented on several points. In the case of CCPs, these additional provisions concerned, firstly, the supervision of third-country central counterparties – in light of Brexit, the objective being to increase the powers of the European authorities over CCPs deemed systemically important for the EU – and, secondly, the applicable framework for recovery and resolution, in order to incorporate into European Union (EU) law the principles adopted by the Financial Stability Board (FSB) in this area. In addition to CCPs, in line with the relevant principles of the CPMI[1] and the IOSCO,[2] and in a context of increasing threats, the Eurosystem has also clarified its expectations regarding the monitoring of cyber risks faced by market infrastructures under its jurisdiction. In the area of retail payments, the primary task was to implement PSD2, which came into force in early 2018, in particular its security aspects, and especially in light of the work of the *Observatoire de la sécurité des moyens de paiement* (OSMP - Observatory for the Security of Payment Means). Finally, in the wake of the work carried out by the G7 in 2019 under the French Presidency and then by the FSB, in late 2020, the European Commission published a legislative proposal on the regulatory framework for crypto-assets, as part of a legislative package on digital finance. The negotiation phase that has begun will refine the substance of the proposed measures as necessary, but in any event the process constitutes a major development that will enable the EU to meet the challenges of new technologies.

The Banque de France's supervisory actions have focused on three main areas. The first priority was – and remains – the continuing assessment of market infrastructures' compliance with the laws that apply to them. The analyses conducted on this issue provide an overview of all risks to which they are exposed (financial, operational, cyber, etc.), as well as the mechanisms in place or the measures taken to prevent these risks, and ultimately serve to ensure both their robustness and their performance. The second, in the field of cashless means of payment, focused on a series of actions designed to enhance their security, whether by providing support to the financial community – supplemented by individual monitoring – for the gradual implementation of strong customer authentication or by analysing the security measures taken by issuers of means of payment. A third priority in 2020 was closer monitoring of both market infrastructures and players in the retail payments chain to ensure their resilience in the face of the operational and other risks created by the COVID-19 pandemic on their information systems and organisations – and it is clear they have been able to cope with them.

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

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

1

OVERSIGHT OF FINANCIAL MARKET INFRASTRUCTURES

OVERSIGHT OF FINANCIAL MARKET INFRASTRUCTURES

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 entities 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

Whereas the two previous periods (2012-2014 and 2015-2017) were marked by the transposition into EU law of the Principles for Financial Market Infrastructures (PFMI) defined in 2012 by the CPMI and the IOSCO,[3] the period under review saw changes reflecting new issues taken into account, particularly the amendments to EMIR, advances in resolution and developments related to the prevention of cyber risks.

1.1 A more stringent CCP regulatory framework combined with adjusted clearing obligations for financial players

EMIR, the European regulation governing these provisions published in July 2012, was amended twice during the period under review. The first amendment, which focused on clearing and reporting obligations and is known as "EMIR Refit", for Regulatory Fitness, aimed to promote proportionate implementation of regulatory requirements in this area, whereas the second, known as "EMIR 2.2", addressed oversight of third-country and European Union CCPs.

The first point led to the publication on 20 May 2019 of Regulation No. 2019/834 (EMIR Refit), which reduces clearing and reporting obligations, in particular for non-financial counterparties, and imposes new requirements on CCPs such as providing financial players with "fair, reasonable, non-discriminatory and transparent" access to clearing services.

The second point, which resulted in Regulation No. 2019/2099 of 23 October 2019 (EMIR 2.2), overhauls the supervisory framework for third-country and European Union (EU) CCPs. This regulation aimed, firstly, to strengthen the control of the systemic risk created by offshore CCPs by introducing a proportionate regulatory and supervisory regime and, secondly, to harmonise the supervision of EU CCPs through an enhanced role for ESMA.

The original regime, which was based on the equivalence of regulatory frameworks, did not permit the European authorities to exercise effective control over CCPs established outside the EU. To remedy this deficiency, which is potentially detrimental to European financial stability, in particular with regard to Brexit, the EMIR review led to the adoption of a three-tier system that classifies CCPs depending on how systemically important they are for the EU:

- Tier 1 CCPs: for non-systemically important CCPs, the current recognition arrangement based on the equivalence of regulatory frameworks will be reviewed regularly and will impose conditions to ensure actual equivalence.

- Tier 2 CCPs: for systemically important CCPs, compliance with EMIR standards will be required and directly verified by ESMA supervision through a new dedicated body, the CCP Supervisory Committee (which also has jurisdiction over EU CCPs).

3 The Banque de France and the *Autorité des marchés financiers* are the French members of the CPMI-IOSCO.

- In addition: the Commission is granted discretion to refuse recognition of clearing activities deemed of "substantial systemic importance", on the recommendation of ESMA and with the agreement of the relevant central banks (EMIR Article 25(2c)). If recognition is refused, the relevant business segments must relocate to the EU in order to continue to offer services to European entities.

The delegated acts specifying this three-tier system, which the Commission published in September 2020, show that only the UK CCPs LCH Ltd and ICE Clear Europe will be subject to the Tier 2 supervision regime. At the same time, the European authorities have stressed the need for European financial players to reduce their exposure to these CCPs by June 2022, the expiry date of the temporary equivalence period the European Commission granted the United Kingdom. In addition, ESMA has publicly undertaken[4] to carry out, by the first half of 2022, a comprehensive review of the systemic importance of these two CCPs for the European Union and, if necessary, to initiate proceedings under Article 25(2c) of EMIR 2.2 (which may lead to the total or partial non-recognition of the most systemically important central counterparties).

For CCPs established in the EU, supervisory competence will remain at national level. However, ESMA's role has been strengthened (drafting of new technical guidelines and standards, mandatory ex-ante opinion on certain CCP projects) to encourage greater convergence of national approaches. Accordingly, the CCP Supervisory Committee, which was established in early 2020 and which includes all competent national authorities responsible for supervising CCPs, has already acquired a central role in the harmonisation of European CCP supervision practices due to its mandatory involvement in a certain number of matters (e.g. changes to margin models, introduction of new products, control of mergers and acquisitions).

1.2 Recovery and resolution of central counterparties: a clearer international framework and a European framework nearing completion

A clearer international framework

The recovery of a financial market infrastructure 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 of a magnitude that exceeds the capacity of the usual loss absorption mechanisms (in particular, the margins collected by the CCPs and their default funds). Market infrastructures may suffer two main types of losses: losses due to a member's default and losses unrelated to a default (internal fraud, external fraud, losses on the infrastructure's own investments, etc.). Recovery is the responsibility of infrastructures themselves, which must provide for recovery measures in their internal rulebooks. In contrast, resolution is initiated and carried out by the resolution authorities, in particular if the recovery phase has failed or needs to be interrupted on financial stability grounds, and aims to wind down operations in an orderly manner, avoiding the use of public funds as much as possible.[5]

Due to the systemic importance of CCPs, and the particular financial issues raised by the recovery and resolution of these infrastructures, the FSB deemed it necessary to extend recovery and resolution measures to this type of entity so as to cover all foreseeable crisis scenarios, even if unlikely.

In late 2014, the FSB adopted recommendations on the resolution of CCPs.[6] In addition, on 5 July 2017[7] it published guidance on establishing a harmonised framework at the international level, under which, in order to ensure orderly resolution, the authorities will have extensive tools and powers (partial or total contract tear-up powers, forced allocation of open positions or losses, etc.). To regulate the exercise of these powers, the guidance endorses, firstly, a principle of equity in allocating losses (*pari passu*), 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 resolution than in 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 that will be needed to achieve resolution objectives (resolvability assessments).

The guidance requires adoption of resolution plans for all systemically important CCPs, based on close cooperation between the relevant authorities within a jurisdiction (between resolution and supervisory authorities) and internationally (establishment of Crisis Management Groups (CMG)).

This work of the FSB continued after 2017 with the negotiation of guidance (published on 16 November 2020) on two aspects. The first aspect, concerning adequacy of resources, is to define a five-step process to be followed by the resolution authorities of systemically important CCPs in order to analyse the nature, availability and amount of resources within the CCP in the event of resolution and, in the event of insufficient resources, to consider the possible use of additional resources through enhanced statutory powers.

Secondly, the guidance was originally intended to clarify the treatment of CCP shareholders in resolution cases. This is because CCPs are subject to particular tension in this area: on the one hand, the Key Attributes of the FSB and the 2017 Guidance endorse the fundamental resolution principle that shareholders must absorb losses but, on the other hand, the CCPs' contractual rules provide that equity only absorbs a limited share of losses (the CCP's "skin in the game", currently set at 25% of equity in the EU). The negotiations were unsuccessful in producing a compromise within the FSB on this issue, which may ultimately be left to the resolution authorities in each jurisdiction.

A finalised European framework

At European level, in late November 2016, the European Commission published a draft regulation on the recovery and resolution of CCPs. Negotiations were temporarily suspended in 2018 pending the finalisation of EMIR 2.2 and international work at the FSB, but resumed in 2019 and concluded in the summer of 2020, with publication in the OJEU scheduled for early 2021. This regulation aims to transpose international standards into EU law. It therefore includes the main conclusions of the FSB's Key Attributes: providing a framework for the measures CCPs adopt in their recovery plans, granting resolution authorities the powers necessary to resolve a non-viable CCP and defining appropriate resolution tools. The aim is to avoid using public funds, except as a last resort.

In general, the regulation provides for increased shareholder liability, particularly if losses are not due to a default (and are therefore purely attributable to the management of the CCP), without however absolving participants of their contribution to the losses. The framework thus defined is due to be refined by regulatory technical standards that will be drawn up starting in 2021.

1.3 Amendment of the regulation on systemically important payment systems

Regulation (EU) No. 795/2014 of the ECB of 3 July 2014 (the "SIPS Regulation") on oversight requirements for systemically important payment systems (SIPS) was amended for the first time in 2017 by Regulation (EU) No. 2017/2094 of the ECB of 3 November 2017. This amendment clarified existing obligations, added new risk management requirements (in particular concerning cyber resilience) and expanded the powers of the authorities.

The operators of the four SIPS were given a 12-month period to comply with the amended regulation (18 months for the provisions on financial obligations). Following the self-assessment required of the operators, the competent authorities (Banque de France for CORE(FR), the ECB for TARGET2, EURO1 and STEP2-T) conducted a gap assessment to determine whether the SIPS fully complied with the new requirements. This assessment phase was completed in July 2020.

During this assessment phase, on 4 May 2020, the Governing Council identified Mastercard CMS as a SIPS. This new SIPS will be overseen by two competent authorities (the ECB and the National Bank of Belgium).

The SIPS Regulation will soon be amended again, in particular to specify the procedures for joint oversight by two competent authorities. This amendment will also detail and clarify the procedure for designating a payment system as a SIPS.

1.4 The "CSDR" European regulation harmonising securities settlement and strengthening the operating framework for central securities depositories

Regulation (EU) No. 909/2014, which aimed to harmonise, in the European Union, the requirements for securities settlement and for organising and conducting the activities of central securities depositories ("CSDR"), came into force in 2014.

In 2017, this regulation was supplemented by a series of technical standards covering, for example, the requirements governing the operation, authorisation and supervision of central securities depositories (CSD). Another technical standard adopted in May 2018, Commission Delegated Regulation (EU) No. 2018/1229 on settlement discipline, which should have entered into force 24 months after its publication (25 May 2018), was postponed a first time to 1 February 2021 and a second time to 1 February 2022 (on 28 August 2020, ESMA published a report on a further postponement of the date of entry into force of Commission Delegated Regulation (EU) No. 2018/1299 on settlement discipline to 1 February 2022).

4 *https://www.esma.europa.eu/press-news/esma-news/esma-recognise-three-uk-ccps-1-january-2021*

5 *https://www.bis.org/cpmi/publ/d00b.htm?&selection=156&scope=CPMI&c=a&base=ter*

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

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

In France, the AMF and the Banque de France are the competent authorities under CSDR and jointly supervise CSDs established in France. The Banque de France's responsibilities focus primarily on settlement finality, cash settlements, links between CSDs, operational risk and investment policies.

Most European CSDs have now been authorised (22 out of 30) and several procedures are underway with respect to the others. Of the CSDs that have been authorised, two are French: Euroclear France and ID2S.

After authorisation, CSDR requires the competent authorities, at least once a year, to review the arrangements, strategies, processes and mechanisms implemented by the CSDs and to evaluate the risks to which the CSDs are exposed. The level of detail and frequency of this evaluation are determined by the competent authorities depending on the size and systemic importance of the CSDs, as well as the nature, scale and complexity of their activities. The competent authorities must inform the relevant authorities (in particular the Eurosystem) of the results of the review and evaluation.

Since 2020, and in accordance with the provisions laid down in CSDR, a process for amending the regulation has been launched. The work currently consists of identifying the matters to be covered and defining the general approach of this first amendment. At this stage, there is not yet a legislative proposal for an amendment to CSDR (the timetable for which is unclear at this time).

The Commission's timetable is divided into two phases:

- a first stage (for which the Commission is expected to submit a report on 16 December 2020) that includes matters selected to be covered first because they should be simpler to deal with: cross-border activities/passports; internalised settlement; conducting regular reviews (post-authorisation) of the compliance and risks of CSDs; new technologies, although it is still uncertain whether amendments can be made on this point at this stage because, at the same time, the Commission is undertaking a certain amount of work on innovation. In fact, this matter is expected to be addressed in connection with the new draft Commission regulations published on 24 September 2020, in particular on crypto-assets (MiCA) and a "pilot regime" to allow experiments with derogations from certain CSDR provisions (*see box below*).

- a second stage, which is expected to start in 2021, during which the Commission will initiate a more exhaustive review of CSDR, broadening its scope beyond the issues previously identified. The list of matters to be analysed has not yet been fully defined.

1.5 Implementation of new international cyber resilience standards

More than ever, cyber threats engender major resilience challenges for the financial system and, in particular, for market infrastructures. Therefore, work to improve cyber resilience continues in two areas:

- a paradigm shift due to, firstly, the ever greater means available to malicious organisations and, secondly, the growing complexity of information systems and the increased number of channels used to access them. As a result, securing information systems is complex, in a context of heightened cyber risk that makes it essential to be able to react optimally in the event an incident occurs;

- taking into account the growing operational interdependence between the various financial players and the use of third-party suppliers, some of which have become critical for the financial sector as a whole and market infrastructures in particular. This has led to an awareness that a failure of the weakest link can impact the entire financial sector.

The objective is to ensure that all players deploy a level of protection appropriate to the threats that covers all areas of cyber security, from the identification of risks to business recovery plans and including incident detection and intrusion testing.

Adapting international and European laws

At international level, the G7 member countries continued the work begun in 2016 with the publication in October 2018 of Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector and Fundamental Elements for Threat-led Penetration Testing.

- The Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector apply to both financial entities and financial sector regulators. They stress the key elements to be taken into account when selecting suppliers and, thereafter, when monitoring the services provided, while highlighting the importance of integrating these suppliers into the incident response, continuity and disaster recovery systems in the event of a major incident. Particular emphasis is also placed on identifying third-party suppliers that may present a systemic risk for the

financial sector as a whole due to the critical nature of the services they provide and the large number of players to which they provide them.

- The Fundamental Elements for Threat-led Penetration Testing provide key principles financial entities should follow when they conduct this type of testing. Particular emphasis is placed on coordination between the financial authorities of the various countries concerned when multinational entities conduct international tests.

The Eurosystem used the CPMI-IOSCO Guidance on Cyber Resilience for Financial Market Infrastructures, which was published in late June 2016, as the basis for the assessment it undertook of the cyber resilience of European financial market infrastructures, with a view to strengthening it.

This work consisted of:

- applying the CPMI-IOSCO Guidance to set out, in a document published in December 2018, the expectations of European supervisors with regard to the cyber resilience of payment systems and market infrastructures (cyber resilience oversight expectations (CROE) for financial market infrastructures);

- promoting dialogue between regulators and industry: the European Cyber Resilience Board is a strategic high-level meeting created in March 2018 between regulators and industry representatives on the issue of the cyber resilience of financial market infrastructures and critical service providers. A first major achievement of the meeting was the launch in February 2020 of a platform for exchanging crucial information on the evolution of cyber threats (Cyber Information and Intelligence Sharing Initiative, or "CIISI-EU"), which aims to protect the European financial sector by enhancing prevention, detection and the ability to respond to cyber attacks;

- creating a harmonised framework for carrying out red-teaming intrusion testing:[8] the work begun in early 2017 led to the publication in May 2018 of the Threat Intelligence-based Ethical Red Teaming (TIBER-EU) framework, which harmonises the procedures for cyber penetration testing in the financial sector. These penetration tests play an essential role in assessing the ability of the entity tested (market infrastructure, bank, insurer, critical service provider, etc.) to protect itself and detect and respond to an advanced cyber attack. This TIBER-EU framework, which is intended to be used by the authorities, as well as by operators and the specialised companies whose services they will use, places particular emphasis on facilitating international tests and the mutual recognition thereof by the various relevant financial authorities.

Lastly, the Banque de France participated in the public consultation conducted by the European Commission between December 2019 and March 2020 on the operational resilience of financial sector players to cyber attacks. The public consultation collected stakeholders' views on the need to improve the legislative acquis on:

- security risk management requirements, in particular in relation to information and communication technologies (ICT);

- incident reporting;

- operational and IT resilience tests;

- oversight of third-party ICT providers that provide services to financial institutions.

Organisation of an international crisis simulation exercise

It is now widely acknowledged that the extensive interconnection of the various financial centres worldwide requires the financial authorities to adopt a harmonised strategic approach to cyber security. In particular, the various fundamental elements published by the G-7[9] have shown that proper coordination of response and recovery actions in the event of a major cyber security incident is one of the key elements of the financial sector's operational resilience. Several jurisdictions already carry out regular national and regional exercises, at the European level for example, but no large-scale exercise had yet been organised at the global level for the financial sector.

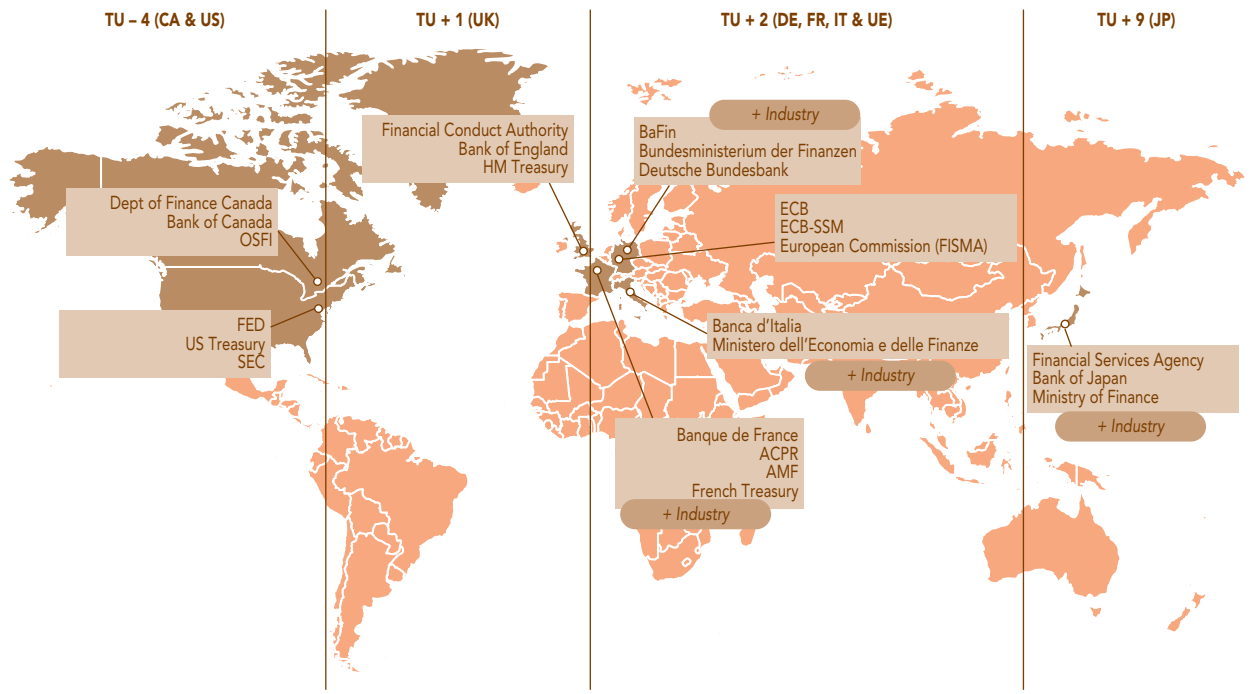
That is why, in October 2017, the G-7 finance ministers and central bank governors approved the French proposal, made ahead of France's presidency of the G-7 in 2019, to organise a cyber exercise involving the financial authorities – finance ministries, central banks, banking authorities and market authorities – of the relevant countries.

The Banque de France was entrusted with organising the exercise and coordinating the preparatory work.

8 Red teaming: exercises and simulations in which the opposing team (the "red team"), like cyber attackers, attempts to break through the defences of the targeted entity.

9 See previous chapter.

Participants in the G-7 Cross-Border Coordination Exercise of June 2019



Source: Banque de France.

The exercise, which was carried out in real time over a period of three days in June 2019, simulated a major cyber incident impacting several financial sector players simultaneously. Twenty-four G7 financial authorities took part, as well as representatives of the financial sectors in France, Germany, Italy and Japan.

The exercise served to validate, at the international level, the communication protocol in place between the G7 financial authorities, in particular its capacity to facilitate exchange of the most incident-relevant information, enable the coordination of responses and ensure the most effective and coordinated recovery of financial services. In France, it also served to validate the resilience of the national crisis coordination system set up in connection with the Paris Resilience Group (*Groupe Robustesse de Place*) and to assess the adequacy of the contingency measures available.

This exercise, which by nature was very complex and was the first of its kind at the global level, marked a major step forward in terms of international cooperation. Thanks to its success, the G-7 authorities have agreed to establish a programme of exercises for the coming years and to publish in the near future the Fundamental Elements of Cyber Exercise Programmes.

1.6 International work of the CPMI-IOSCO

This work focused primarily on a) monitoring implementation of the PFMI and b) further developing certain issues they cover.

Monitoring implementation of the PFMI

This work follows a three-level approach:

- At the first level (L1), each jurisdiction conducts a self-assessment of the progress of transposing the PFMI into local law. Because most jurisdictions now deem that they have transposed the PFMI, the work is now focused on the next two levels.

- At the second level (L2), the extent to which the legislative measures adopted in the various jurisdictions completely transpose the PFMI is assessed. Since 2017, the Implementation Monitoring Standing Group (IMSG – the CPMI-IOSCO working group that monitors implementation of the PFMI) has carried out assessments of Switzerland, Canada and the United States (payment systems and CSDs), and the assessments of Brazil, Turkey and the European Union (payment systems and CSDs) are being completed.

- At the third level (L3), the consistency of market infrastructures' implementation of the PFMI is assessed. The risk management practices and recovery plans of CCPs, and their implementation of "cover 2" (scaling of reserves to cover the simultaneous default of their two largest members) were assessed in 2019. The infrastructures' continuity plans were assessed in 2019 and 2020, and an assessment of their cyber risk management was launched in 2020.

Although the PFMI have unquestionably become the international benchmark for oversight of market infrastructures, how robustly they are implemented varies from one jurisdiction to another. The IMSG's level 2 work, which is now focusing on jurisdictions where financial markets are less developed and internationalised, has found that the legal vehicles used to "transpose" the PFMI vary widely. The level 3 work also highlights interpretations of certain PFMI terms or requirements that vary at times. The public reports that will be produced on each issue studied will lead to a gradual convergence of interpretations and practices by market infrastructures, a key factor in the consistent implementation of the PFMI across the various jurisdictions.

Changes in international standards

The work carried out in this respect focused primarily on:

- the auctions conducted by CCPs to deal with the default of one or more of their members. The studies carried out on this issue resulted in a publication that highlights a diversity of practices and makes clear that improvements could be made (see box);

- the framework for international cooperation between authorities. This involved reviewing the current approaches with regard to the PFMI (and more specifically the principles set out in "Responsibility E"). The lessons learned from this review led to the publication in December 2019 of a report taking stock of the situation and reiterating the need for supervisors of market infrastructures that engage in cross-border activities to be able to exchange information seamlessly in both normal times and crisis periods, in a variety of ways (e.g. by establishing oversight colleges);

- the procedures through which non-banking entities such as insurance companies and funds directly access CCPs ("sponsored" access), in connection with studies previously conducted on the client clearing market. This work, which was begun in 2019, is expected to be completed in 2021 in the form of a report on the benefits and risks of this type of model.

2 Review of oversight of financial market infrastructures

The period under review was marked by the emergence in 2020 of the health crisis caused by the COVID-19 pandemic, which required market infrastructures to adapt rapidly starting in March (massive use of teleworking, rapid change in volumes handled by infrastructures, upsurge of cyber attacks, etc.). All these direct and indirect impacts were closely monitored to prevent a deterioration in the performance of infrastructure services. The overall assessment is that the infrastructures, in particular due to the supervisory frameworks applicable thereto, successfully weathered these various sources of disruption and continued to serve the financial markets satisfactorily.

2.1 LCH SA

LCH SA, the French central counterparty (CCP), offers clearing services for financial instruments and guarantees the 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 €GCPlus, a repo clearing service for which collateral is managed on a tri-party basis by Euroclear France;

- OTC-traded EUR- and USD-denominated credit default swaps (CDS) based on indices or single reference entities.[10]

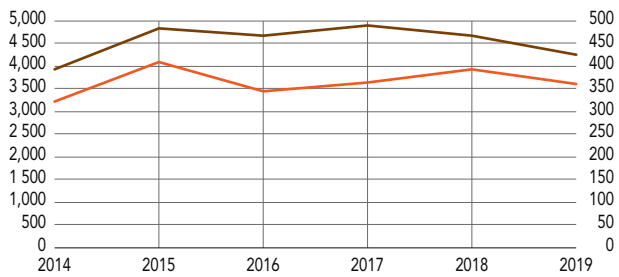
Recent changes and development projects

In the cash and derivatives segment, LCH SA continued and consolidated its clearing offering for the Euronext regulated market in 2020 by supporting the development of Euronext's business (connection to the Oslo stock exchange, the Optiq market platform and Euronext Dublin), and by connecting to other market platforms such as Turquoise (owned by LSEG). In the listed derivatives segment, it now

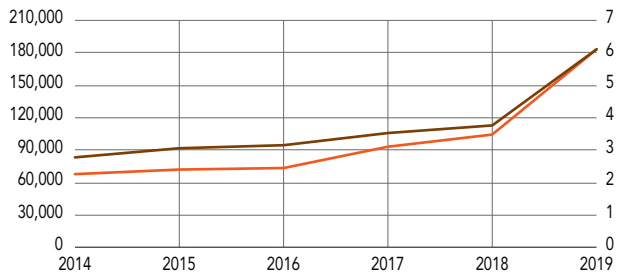
10 Cleared index CDS include iTraxx Europe Main, iTraxx Europe Crossover, iTraxx Europe Senior Financials (and the corresponding single names), CDS iTraxx Europe Subordinated Financials, CDX North America Investment Grade and CDX North America High Yield (and the corresponding single names).

C1 Volumes cleared by LCH SA
(left-hand scale: notional amount in EUR billion, right-hand scale: number of transactions in millions, except for CDS - Chart d - in units)

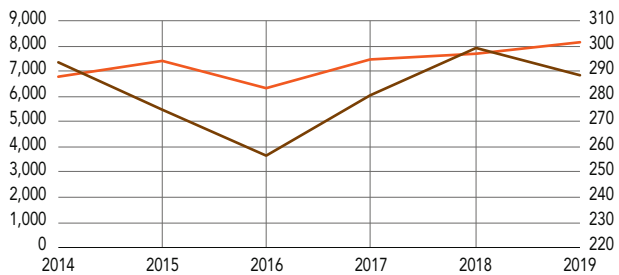
a) *Cash equities*



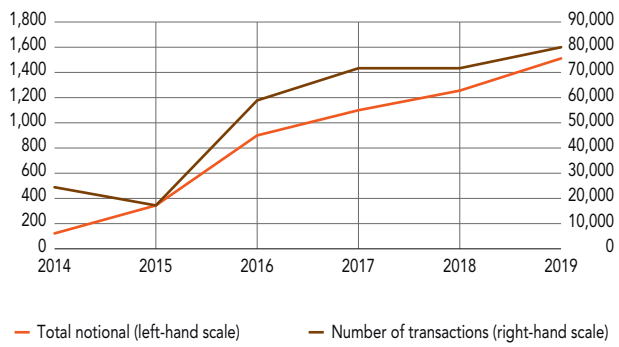
b) *Repo* (*sale and repurchase agreement*, opération de pension)



c) Listed derivatives



d) CDS (*Credit default swaps*)



Source: Bank for International Settlements (BIS) , Statistics on payment, clearing and settlement systems in the CPMI countries (Red Book) 2019.

offers clearing on new contracts: total return futures on the CAC 40 since October 2018, market-on-close futures and index futures on Paris real estate since June 2019.

The CCP's risk models have been modified with the introduction of an additional margin for the de-netting of products that have been settled and delivered. The number of buy-ins has been reduced due to the switch to trade date netting (recycling of outstanding instructions by the CSD, Euroclear France, and no longer by the CCP itself).

In the case of the clearing activity in the bond segment (public debt securities and repos), 2019 was marked by the migration of the euro clearing business from LCH Ltd, which led to an increase in volumes cleared and margins collected. LCH SA's range of services has therefore been extended to new euro-denominated debt. Furthermore, supranational entities now have a specific special member access model to LCH SA services in the bond segment, which the European Investment Bank has been using since 2020.

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

- subordinated financials CDS (indices and single names), in 2018;
- senior non-preferred CDS in single names that are constituents of the iTraxx Europe and iTraxx Senior Financials indices, in 2018;
- monolines representing single names in indices that LCH SA can already clear;
- swaptions or options on US indices (CDX HY, CDX IG), thus complementing the offer of options on 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 30% of euro-denominated CDS cleared in Europe.

Evaluation

The competent national authorities for LCH SA are the Banque de France, the ACPR and the AMF, which exercise joint supervision as competent authorities under EMIR (see section 1.1). LCH SA, which is also a credit institution and, as such, is supervised by the ACPR, is classified as a "less significant institution" and, therefore, is subject

only to indirect supervision by the ECB under the Single Supervisory Mechanism.

In performing their supervisory duties, the competent national authorities perform records-based assessments – for example, reviewing proposals and changes that the central counterparty is planning, analysing information and data on activity and risks, and holding regular meetings with the central counterparty's representatives. The ACPR may also carry out on-site inspections.

Pursuant to Article 18 of EMIR, the French supervisors must also include other European national authorities with an interest in the infrastructure's proper functioning in a college of supervisors (the "EMIR college"). In addition to the authorities responsible for supervising the infrastructure, these colleges include the supervisors of the main clearing members, trading venues, CCPs with which interoperability arrangements have been established, central securities depositories and central banks of issue of the main European Union currencies cleared, as well as the European Securities and Markets Authority, which has no voting rights.

The aim of this system is to promote a standardised approach to implementing EMIR requirements in the European Union and an appropriate evaluation 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 European Union member countries. The college of authorities is the appropriate forum for exchanging information about the CCP and assessing changes that it proposes. LCH SA's EMIR college was set up in January 2014 and includes 19 authorities (including ESMA) from nine different European Union countries. The Banque de France chairs the college. College meetings provide an opportunity to exchange 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 and changes submitted for their review.

In accordance with Article 19 of EMIR, the college's opinion is required, expressed by a vote, not only when a CCP is authorised, but also on proposals to expand service offers or initiate new business lines and on matters with a material impact on the CCP's risk management system, such as a change to its margin model. Under EMIR 2.2, ESMA must also express an opinion on connections to a trading venue, governance changes, outsourcing and interoperability agreements.

The French authorities hold a meeting of the college every year and, therefore, three meetings were held between 2018 and 2020.

When the United Kingdom's exit from the European Union becomes fully effective on 1 January 2021, the Bank of England will cease to be an ex officio member of the EMIR college for LCH SA. However, given the very close ties between the French CCP and LCH Ltd, the UK's CCP, it will be necessary to continue to involve the UK authorities in the collegial supervision of LCH SA. The French authorities are currently studying various options for modifying the body that supervises LCH SA, in particular in connection with the review of ESMA standards on the functioning of the colleges.

2.2 Euroclear France and ESES France

Euroclear France, a central securities depository (CSD), offers the three "core services" defined by CSDR[11] (see section 1.4), as well as several "non-bank ancillary services"[12]. Euroclear France operates the ESES France securities settlement system[13], which has been connected to T2S since September 2016. Nearly all securities transactions and trades transit and are processed via T2S, to which Euroclear France, a member thereof, outsources the securities settlement service. ESES France members have a contractual relationship with Euroclear France only, whether they are technically T2S directly connected parties or indirectly connected parties.

Since 2010, Euroclear Nederland and Euroclear Belgium have outsourced operational management of their securities settlement and delivery business to Euroclear France. ESES France processes about 90% of the securities settled by the three ESES CSDs (Euroclear France, Euroclear Nederland and Euroclear Belgium). Based on the most recent ECSDA data[14], Euroclear France accounts for around 12% of securities in custody and 10% of securities transactions settled in Europe. The value of the 93,000 securities in custody in 2019 was EUR 7,322 billion (up 12%). The value of settlement and delivery instructions in 2019 was EUR 112,464 billion.

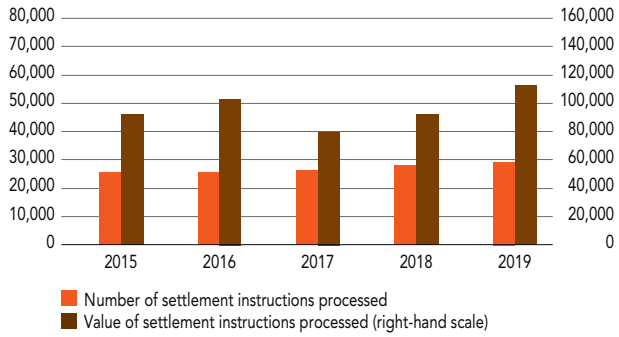
11 a "notarial service" for the issuance of securities, a "central maintenance service for securities accounts" and a "settlement service" via the operation of a securities settlement system

12 managing securities transactions (payment of coupons and dividends, etc.), assigning ISINs to new securities issued and tri-party collateral management

13 Euroclear Settlement of Euronext-zone Securities

14 *ECSDA - European Central Securities Depositories Association.* https://ecsda.eu/

C2 Number and value of settlement and delivery instructions processed by ESES France
(left-hand scale: number in thousands; right-hand scale: value in EUR billions)



Note: ESES, Euroclear Settlement of Euronext-zone Securities.
Source: Banque des règlements internationaux (BRI – BIS Statistics Explorer) – Statistics on payment, clearing and settlement systems in the CPMI countries (Red Book), 2019.

Oversight framework

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 powers conferred on it by the *Code monétaire et financier*[15], but it is also the competent national authority for the French central securities depositories. This status is shared with the AMF, which was already the supervisory authority of Euroclear France under the previous national oversight framework.

The securities settlement systems (SSS) and the three CSDs, Euroclear France, Euroclear Belgium and Euroclear Nederland, are jointly supervised at ESES level under a cooperation arrangement between the French, Belgian and Dutch authorities. This supervision is part of the broader framework established by the memorandum of understanding entered into force in July 2011 between the authorities with jurisdiction over ESA,[16] which defines the procedures for cooperation and exchange of information between the authorities with respect to the regulation and supervision of securities settlement and delivery transactions. The National Bank of Belgium has been designated to coordinate the cooperation. However, each ESES competent national authority retains its powers with regard to its national CSD. This cooperation mechanism is currently being reviewed in order to incorporate the new provisions introduced by CSDR aimed, in particular, in the case of ESES CSDs, at strengthening cooperation and coordination measures between supervisory authorities.

Application of CSDR

Euroclear France, like the other two ESES CSDs, was authorised under CSDR in April 2019. It was authorised by the AMF upon consultation with the Banque de France.

In 2020, in accordance with the provisions of CSDR, Euroclear France underwent an initial annual review and evaluation procedure, which was conducted by the authorities and covered the period from April 2019 to March 2020.

ESES France is a Eurosystem-eligible securities settlement system and, therefore, can be used for monetary policy operations conducted by the Banque de France.

2.3 ID2S

ID2S is a new French central securities depository that was authorised under CSDR in October 2018. It operates the Rooster Securities Settlement System (RSSS). In August 2020, RSSS became eligible for Eurosystem operations settlement following a review of its compliance with the eligibility criteria and, therefore, it can be used for Eurosystem monetary policy operations.

ID2S incorporates blockchain technology into its information system, instead of a traditional database model that lists the information required for CSD activity. This is a private blockchain enabling it to validate all transactions.

The CSD, which has been connected to T2S since late October 2018 (enabling the settlement of transactions in central bank money), offers the three core services defined by CSDR: a notarial service for the issuance of securities, a central maintenance service for securities accounts, and a securities settlement service to enable the circulation of securities.

ID2S currently handles only negotiable debt securities, more specifically NEU CPs, which are short-maturity securities (one year maximum) that may be issued by financial or non-financial companies and by public bodies.[17] It may eventually extend its activity to other securities, in particular euro commercial paper ("EuroCP"), another type of negotiable debt security issued by governments, public institutions and companies, that is mainly traded in London.

2.4 CORE(FR) and SEPA(EU)

CORE(FR) and SEPA(EU) are two retail payment systems operated by STET SA (*Systèmes Technologiques d'Échanges et de Traitement*).

CORE(FR)

CORE(FR) allows its participants, which are French banks, to combine and submit domestic retail transactions for settlement of their net balance. In August 2014, the ECB Governing Council designated CORE(FR) a systemically important payment system, together with the pan-European systems TARGET2, EURO1 and STEP2-T. In fact, CORE(FR) meets two of the four criteria set by Regulation (EU) No. 795/2014 of the ECB on oversight requirements for systemically important payment systems, i.e. the daily value of payments processed by the system (over EUR 10 billion) and its market share of the total volume of euro-denominated payments.[18] These criteria were not changed by the new Regulation (EU) No. 2017/2094 of the ECB of 3 November 2017.

Following the ECB's decision, the Banque de France was designated as the competent authority for CORE(FR); it is currently the only Eurosystem national central bank with sole supervisory authority over a systemically important payment system.

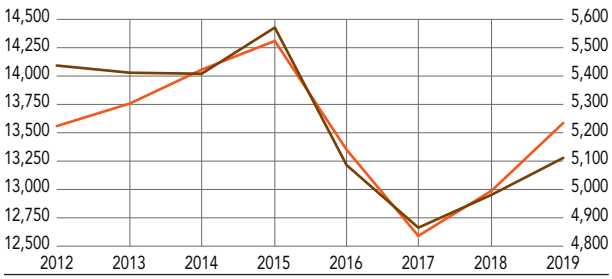
Historically, CORE(FR) processed all cashless means of payment, before the switch to the new SEPA(EU) system (see below). To date, CORE(FR) continues to process the majority of means of payment that are settled daily in order to calculate the net balance of each participant. Multilateral net positions are settled daily at approximately 3.00 p.m. in TARGET2-Banque de France.

Activity

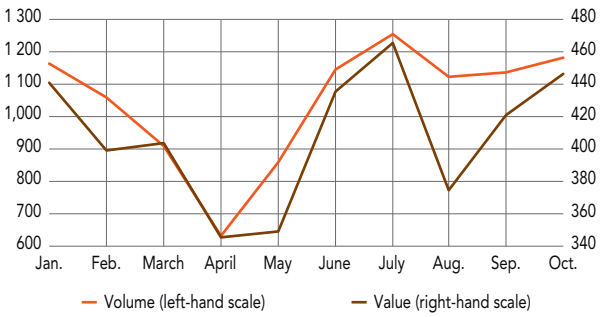
In 2019, about 13.5 billion transactions, with a value of nearly EUR 5,112 billion, were cleared in CORE(FR), making CORE(FR) the leading retail payment system in terms of volumes processed. From 2017 to the end of 2019, the transactions cleared in CORE(FR) grew in volume by approximately 7.9% and in value by 5%, after having fallen in 2016 due to the migration of direct debits to SEPA(EU). From January to October 2020, between 631 million and 1,251 million transactions were settled monthly, representing values of between EUR 345 billion and EUR 466 billion. The significant differences in volumes processed in 2020 is explained by the impact of lockdown, which severely curbed credit card activity in March, April and May.

C3 Activity in CORE(FR)
(left-hand scale: millions of transactions; right-hand scale: EUR billions)

a) Annual activity



b) Over the first 10 months of 2020



Source: Banque de France, STET, authors calculations.

As a SIPS, CORE(FR) set up a financial safety mechanism due to the significant number of transactions it processes each day. This financial protection mechanism takes the form of a mutual guarantee fund (nearly EUR 600 million since 28 November 2019), supplemented by individual guarantees to cover the highest net debit position.

Since late February 2013, STET has hosted the *Centre d'Échange et de 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.

15 Article L. 141-4 – II: Pursuant to the duties of the European System of Central Banks, (…) the Banque de France shall ensure the security of systems for the clearing, settlement and delivery of financial instruments.

16 Countries in which Euroclear SA entities operate: Belgium, France, Netherlands, UK/Ireland, Sweden, Finland.

17 This market concerns around 400 issuers and about 100 institutional investors, with EUR 316 billion in investments at end-June 2020. Three-quarters of trades are concentrated in the primary market, with a predominance of over-the-counter trading intermediated by brokers.

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

Evaluation

In 2016, the Banque de France completed its report assessing the compliance of CORE(FR) with the requirements of Regulation (EU) No. 795/2014 applicable to systemically important payment systems (SIPS Regulation). The system was deemed broadly compliant and the implementation of the action plan was closely monitored by the Banque de France, which reported thereon to the Eurosystem. The closure of the action plan was ratified by the ECB's Governing Council in September 2019 after STET had implemented all the recommendations made.

Regulation (EU) No. 2017/2094 amended certain provisions of the SIPS Regulation. In 2019, a gap assessment was conducted to determine if it was compliant with these new provisions. This included a review of the cyber resilience expectations set out in the CROE.

A comprehensive assessment was conducted again in 2020. It included the measures implemented by the operator in response to the recommendations made in 2019 following the gap assessment. These two exercises concluded that CORE(FR) was broadly compliant with the amended SIPS Regulation.

SEPA(EU)

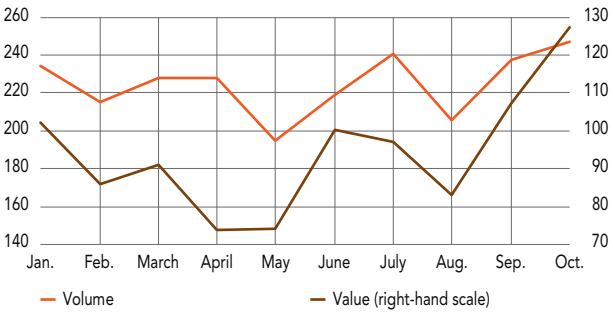
In late 2016, STET launched a second retail payment system. SEPA direct debits (SDDs), which were previously processed in CORE(FR), are now processed and cleared in SEPA(EU). Although legally CORE(FR) and SEPA(EU) are two separate systems, they nevertheless have common characteristics. SEPA(EU) operates on the same technical platform as CORE(FR) and has the same governance structure.

Because SEPA(EU) settles annual 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.[19] This category of payment system is assessed on the basis of its compliance with nine of the CPMI-IOSCO principles for financial market infrastructures (PFMI).[20]

Activities in SEPA(EU)

During the first ten months of 2020, around 2.5 billion transactions (SDD direct debits), with a value of EUR 942 billion, were settled in SEPA(EU). In 2019, the volume of transactions settled was stable on a monthly basis (between 204 million and 249 million transactions per month), and the monthly values settled varied between approximately EUR 84 billion and EUR 122 billion.

C4 Activity in SEPA(EU) in 2020
(left-hand scale: volume in millions of transactions, right-hand scale: value in EUR billions)



Source: Banque de France, STET, authors calculations.

In November 2018, STET launched an instant payment service for the French and Belgian banking communities. CSM Instant Payment is an instant credit transfer settlement service that is based on the "SCT Inst" scheme developed by the European Payments Council.[21] Its ceiling, which was initially set at EUR 15,000 at the interbank level in France and is reviewed annually by the EPC, was raised to EUR 100,000 in July 2020. As of 30 October 2020, 18 payment service providers in France and Belgium were connected to IP CSM, covering 85% of the accounts of those two countries.

This offer was enhanced in February 2020 with the Single Window Instant Payments (SWIP) solution that enables participants to manage their instant payments via a single access point, including when they use the interconnection offered by TIPS or RT1 (instant payment systems operated by the Eurosystem and EBA Clearing, respectively), thus opening up a channel to these two pan-European systems.

Evaluation

Following the SEPA(EU) launch evaluation in July 2017, STET proposed measures in response to the supervisor's recommendations and then implemented the required action plan.

In February 2019, the Banque de France updated the SEPA(EU) evaluation report in light of the PFMI requirements applicable to other retail payment systems (ORPS) in connection with the launch of the instant payment functionality. The system was deemed compliant with the nine principles applicable to it.

A minor change evaluation was also conducted in August 2020, following the launch of the SWIP functionality. This change did not affect the compliance of the system.

2.5 Cooperative oversight

The Banque de France also contributes to the cooperative oversight of various market infrastructures and critical service providers established in other countries and/or with a pan-European or international scope.

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 2020, 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 five other European Union countries that are not members of the euro zone (Bulgaria, Croatia, Denmark, Poland and Romania).

Like the French CORE(FR) system, TARGET2 was identified as a systemically important payment system by a decision of the Governing Council in August 2014. It is therefore subject to the requirements of the amended ECB SIPS Regulation No. 2017/2094 of 3 November 2017. The European Central Bank coordinates the oversight of TARGET2, with the cooperation of the national central banks that participate in the system.

A gap assessment vis-à-vis the amended SIPS Regulation was carried out in 2020 under the direction of the European Central Bank, in conjunction with the central banks of the euro zone that volunteered to contribute to this evaluation procedure. The operator must take several actions to bring the system into full compliance with all provisions of the amended Regulation. The TARGET2 operator has undertaken to implement the requested measures, which the European Central Bank will closely monitor and report on. However, some of these actions may not be completed until the future consolidated technical platform is implemented (see below).

The cyber resilience of the TARGET2 system (Article 15.4(a) of the SIPS Regulation) is the subject of particular attention. The evaluation in progress will be finalised in early 2021. Compliance is assessed in accordance with the cyber resilience oversight expectations (CROE) methodology.

To encourage the development of instant payments in Europe, in November 2018, the Eurosystem launched an instant payment settlement solution with the creation of the TARGET Instant Payment Settlement (TIPS), as a new service within TARGET2. TIPS directly processes instant payments between two of its participants, using a real-time payment procedure.

As a TARGET2 service, TIPS is monitored on an ongoing basis by the Eurosystem. The forthcoming inclusion of new non-euro currencies in TIPS has led to an expansion of its oversight arrangements with the creation of the TIPS Currencies Oversight Group. In addition to the Eurosystem, this group will include the central banks of issue of the currencies that are traded in TIPS, primarily the Swedish krona.

T2S

Although 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 securities settlement platform makes it systemically important. The ECB is the main overseer of T2S, with the active participation of all national central banks, which validate its approach and conclusions. In 2019, T2S settled 154,769,117 transactions (for a total value of EUR 282.06 trillion).

Furthermore, T2S is overseen jointly by the central banks and financial market authorities of the various jurisdictions in which at least one CSD has contractually outsourced its settlement and delivery service to T2S. This cooperative oversight body is co-chaired by the ECB and ESMA. In addition to the 24 CSDs that migrated to T2S during the five initial migration waves, ID2S (a French CSD) and VP Securities (a Danish CSD) migrated on 29 October 2018. In addition to ESMA and the ECB, the T2S cooperative arrangement now comprises 22 central banks and 22 national market authorities from the European Union and the European Economic Area.

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

20 The nine principles in question 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).

21 EPC SCT Inst is a pan-European scheme based on SEPA credit transfers. This set of rules and procedures is intended to prevent the fragmentation of the European retail payment market. The SCT Inst scheme requires transactions to be processed in less than 10 seconds, 24 hours a day, 7 days a week and 365 days a year.

Evaluation of T2S against PFMI requirements

A comprehensive oversight evaluation of T2S against the PFMI requirements, which was begun in 2018, was completed in early 2020. The few recommendations and observations generated by this evaluation were incorporated into an action plan that is being implemented by T2S.

SWIFT

SWIFT (Society for Worldwide Interbank Financial Telecommunication) is the leading global provider of standardised interbank transfer messaging services, particularly in the areas of payments and securities. Due to its international dimension and its key role in financial exchanges, which involve nearly all players in the global financial sector, SWIFT is subject to cooperative supervision governed by an agreement between the central banks of the Group of Ten (G10). The National Bank of Belgium, as lead overseer, coordinates this oversight, in which the Banque de France plays an active role.

In 2016, SWIFT launched the Customer Security Programme (SWIFT CSP) for all its customers. It aims to improve the cyber resilience of infrastructures connected to SWIFT and of financial entities that use its services through requirements concerning mainly cyber security governance, prevention, detection and incident response.

The oversight work during the period under review focused, in particular, on the gradual strengthening of the security requirements of the Customer Security Programme, the measures implemented by SWIFT to ensure its customers' compliance with the requirements of the CSP, the ISO 20022 standard[22] adoption programme and the measures taken to ensure operational continuity and the security of operations during the COVID-19 crisis.

CLS

The CLS system provides payment versus payment (PvP) settlement of payment instructions for spot transactions in the foreign exchange market, certain listed derivatives and currency swaps. Each system participant holds a multi-currency account with CLS Bank International 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. At the end of 2020, 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 the relevant central banks to participate in the oversight of the system and ensure its security and effectiveness. Under this framework, the central banks verify CLS's compliance with the standards applicable to payment systems and financial market infrastructures, and study changes the operator proposes 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.

EURO1 and STEP2-T

Under the aegis of the ECB, as competent authority, the Banque de France participates in the cooperative oversight of the pan-European payment systems operated by EBA Clearing: EURO1 (high-value payment system), STEP2-T (retail payment system for processing SCT credit transfers and SDD direct debits) and RT1 (retail payment system for processing SCT Inst instant credit transfers).

The Banque de France has contributed to various evaluations carried out by the ECB, in particular with respect to the compliance of EURO1 and STEP2-T with the Regulation on Systemically Important Payment Systems, which was amended in 2017 (see section 1.3), and cyber resilience expectations (see section 1.5), as well as to the oversight of action plans, including the action plan developed in connection with the evaluation of RT1, EBA Clearing's pan-European instant payment system.

CCPs established in other European Union countries

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 has participated in the colleges of the Italian CCP Cassa di Compensazione e Garanzia (CC&G), with which the French CCP has an interoperability arrangement, the German CCP Eurex Clearing AG, the Dutch CCP EuroCCP and the British CCP LCH Ltd, as the overseer of the central securities depository (Euroclear France) with which these CCPs have ties. Outside Europe, the Banque de France, along with the ACPR and the AMF, has also participated in the Crisis Management Group of the US CCP CME.

22 ISO 20022 is an ISO standard governing electronic data interchange between financial institutions that is mainly used in the areas of payments and securities

BOXES

❶ The impact of Brexit on central counterparties

The decision of the United Kingdom to leave the European Union and the European Economic Area, which took effect on 1 February 2020, has significant implications for the regulation and supervision of market infrastructures established in the UK. In particular, certain UK CCPs are of very significant systemic importance for the remaining 27 Member States of the European Union, in particular LCH Ltd (which clears 80% of the worldwide market for euro interest rate swaps) and ICE Clear Europe Ltd (which clears 99% of listed short-term euro interest rate derivatives and 70% of European CDS).

The first key point of focus during the negotiation period from 2017 to 2020 was to avoid any "cliff-edge" impacts on central clearing. With this in mind, in 2019, the European and French authorities adopted measures for temporary recognition in the event of a hard Brexit. Although the transition agreement negotiated in late 2019 avoided this scenario and a cliff-edge effect in February 2020, the status of the negotiations made it necessary to renew certain measures in September 2020.

A second issue is the supervision of UK CCPs post-Brexit. Currently, these CCPs are subject to 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 Banque de France, the ACPR and the AMF 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's exit from the European Union and the European Economic Area, in the long run, possible regulatory divergences between the British regime governing CCPs and EU law cannot be ruled out. In addition, the EMIR implementation rules (technical regulations, etc.) may no longer be fully applied in the United Kingdom. Aware of these risks, the European Commission granted the UK regulatory framework temporary recognition (until the end of June 2022). If this recognition was not renewed, UK CCPs would no longer be authorised to provide services to European participants unless they relocated their business, at least in part (in particular, their euro business), to the EU.

On the basis of this equivalence decision, at the conclusion of the tiering process for UK CCPs that ESMA carried out in September 2020, LME Clear was classified as a Tier 1 CCP and LCH Ltd and ICE Clear Europe Ltd were classified as Tier 2 CCPs.

In the medium term, the relocation of the most systemically important segments is also desirable in order to preserve European financial stability because a CCP that executes transactions denominated in euros or in another EU currency, but that is not primarily supervised by a European authority, may take – or be required by its national supervisory authority to take – measures that are not in the interest of the EU's financial stability. This lesson was learned from past experience, in particular during the sovereign debt crisis of the euro zone. All in all, the prospect of Brexit and the risk of divergence from the European regulatory framework highlight the need to relocate to the EU the clearing of EU currency-denominated instruments that are of strategic importance for implementing monetary policy, financing the economy and ensuring financial stability in the zone.

Therefore, in 2021, ESMA will reassess LCH Ltd and ICE Clear Europe Ltd to determine if they are of substantial systemic importance for the European Union. This assessment may result in non-recognition under Article 25 (2c) of EMIR, which would require their activities deemed systemically important to be relocated to the European continent (as well as if equivalence is not renewed).

❷ The European Regulation on the Recovery and Resolution of CCPs ("CCPRR")

Under this new regulation, each CCP will now be required to have a recovery plan and a resolution plan in place, which should help maintain infrastructure functions critical for financial stability in the event of a default, avoiding the use of public funds.

a) Increase in the capital requirement for CCPs as going concerns

The regulation introduces a "second skin in the game" ("SIG", which is a share of the CCP's own resources), which will be used just before the recovery tools, after exhausting the default waterfall, to place a portion of the losses on shareholders at the recovery stage. To address the concerns of the smaller CCPs, which may have difficulties raising additional capital, and to avoid competition issues at the international level, the amount of this second SIG is not pre-established, but must be between 10% and 25% of capital requirements. ESMA and the European Commission are tasked with refining, through regulatory technical standards, the rules governing the calculation of this second SIG, taking into account a series of factors listed in the regulation (e.g. the CCP's activities, its collateral re-investment policy and the incentive structure in its ecosystem).

b) The European Regulation on the Recovery and Resolution of CCPs ("CCPRR") Recovery tools

The recovery plans of European CCPs will be required to include tools for allocating losses to members, such as variation margin gains haircutting ("VMGH") of payments owed by CCPs or partial or full contract tear-ups. In the event of recovery, the CCP will be required to suspend dividends and share redemptions and the supervisor may also suspend variable remuneration.

c) Resolution tools

The regulation provides for six tools. Three tools are also available in the bank resolution framework: the write-down and/or conversion of equity instruments and debt securities, sale of activities and bridge CCPs. The other three tools are cash calls, as well as the VMGHs and tear-ups discussed above.

Notably, the regulation does not contain two controversial tools: (i) initial margin haircutting ("IMH"), which could have created significant exposure for participants and an incentive to leave the CCP if a participant defaults, and (ii) the forced allocation of positions, which could have obliged certain members to take positions that they are incapable of handling (this tool is only mentioned in a recital).

d) Flexibility in the use of resolution powers

The regulation provides for flexibility in the authority's use of resolution tools, in order to be able to deal with situations that, by definition, are difficult to foresee, but that may be of significant consequence in terms of financial stability.

e) No creditor worse off (NCWO) principle

The NCWO principle provides that a creditor should not be treated less favourably in the event of resolution than it would have been in the event of liquidation or strict application of the CCP's rules (the "counterfactual"). For CCPs, this corresponds to a failure of the recovery plan that results, (i) in a scenario where one or more clearing members default, in the full tear-up of the contracts of the clearing service whose default management process has failed, and (ii) in a scenario where losses are not due to the default of a clearing member, in the liquidation of the CCP. The "replacement costs" of contracts in the event of a full tear-up must be taken into account to reflect the value the resolution authority preserves by continuing such contracts. They will be defined by a technical regulatory standard proposed by ESMA and adopted by the European Commission, based on the most objective criteria possible.

f) Compensation of participants who suffer losses in resolution

The final regulation grants the resolution authority the power to require the CCP to compensate members who were required to contribute to the resolution beyond their contractual commitments, within the limits permitted by applying the NCWO principle.

g) The European Regulation on the Recovery and Resolution of CCPs ("CCPRR") Recovery and resolution governance in the European Union

The regulation provides that the EMIR colleges set up to authorise CCPs will approve the CCPs' recovery plans and that the CCP resolution colleges will approve their resolution plans. In the event of disagreement within the colleges, the competent authority or the resolution authority, respectively, would make the final decision. A simple majority can refer the matter to ESMA. All powers conferred on ESMA will be exercised by the Resolution Committee created by the regulation.

❸ The draft Pilot Regime Regulation (PRR) for market infrastructures

Adapting regulations to the new challenges created by innovation (in particular, the role of fintechs) seems essential to position the Europe of the future and benefit the economy, citizens and companies.

On 24 September 2020, as part of its digital finance package, in addition to specific provisions on crypto-assets (MiCA) and the digital operational resilience of the financial sector (DORA), the European Commission proposed a pilot regime for market infrastructures using distributed ledger or blockchain technologies.

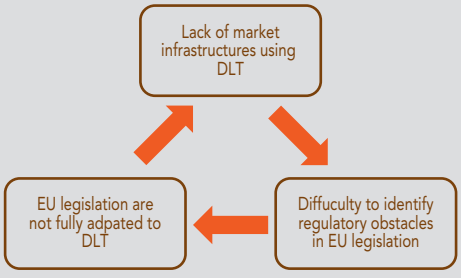
The draft Pilot Regime Regulation (PRR) furthers the Commission's goal, while ensuring financial stability, investor protection and market integrity, of breaking a cycle in which changes to the legislative framework allowing the use of innovative technologies lagged, because the development of these technologies was being hampered by legislative obstacles:

The objective of the pilot regime is therefore to enable the development of a secondary market for crypto-assets and the possibility of testing the use of innovative technology (i.e. blockchain and, more broadly, distributed ledger technology (DLT)) in securities settlement.

The regulation, currently under discussion, proposes a regime that would grant temporary exemptions from some of the obligations ordinarily applicable to two types of players: multilateral trading facilities (MTFs) and securities settlement systems (SSSs) – which are generally operated by CSDs. The exemptions would only apply to MTFs and SSSs that use innovative technologies and demonstrate a genuine need, with the authorisation of their competent authority and on the advice of ESMA.

The pilot regime also covers a broad range of financial instruments, other than sovereign debt. More specifically, it concerns illiquid securities, subject to two conditions: the issuer's capitalisation must be less than EUR 200 million, and bonds are eligible only if the issue amount is less than EUR 500 million. In addition, the PRR sets overall maximum amounts for each experiment (the total value of the securities must not exceed EUR 2.5 billion), above which transition plans will be triggered to return to the traditional framework.

At this stage, the major point under discussion is the position the proposal will take on the principle of giving priority to settlement in central bank money (as recommended by the PFMI), in particular so that the experiments are carried out preferably in digital central bank money and, only if it is not practical and available, in digital commercial bank money. This is also necessary to ensure that the PRR is properly coordinated with the experiments currently being conducted by central banks, including the Banque de France, on a digital central bank money for large-value interbank settlements.

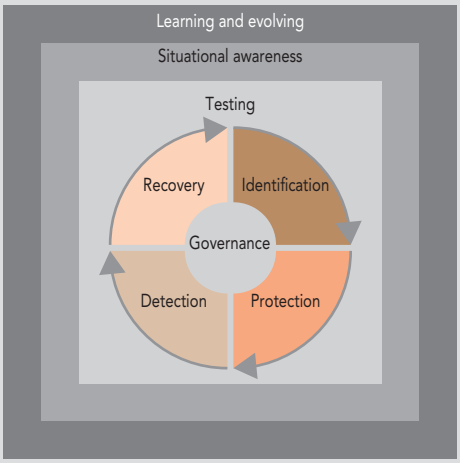


Source: Commission européenne.

❹

Cyber resilience oversight expectations (CROE) for financial market infrastructures

To assess the maturity of European market infrastructures in terms of cyber resilience on the basis of a common European framework, and to monitor their development over time, the Eurosystem drew on the CPMI-IOSCO Guidance published in 2016 to establish a set of requirements. Based on the eight principles of cyber resilience[1] and on best practices in each area, this framework of nearly 300 criteria sets out the expectations of overseers in a more detailed and concrete manner and indicates avenues for longer-term progress by market infrastructures. In line with the logic and scope of the CPMI-IOSCO Guidance, assessing the level of maturity becomes more transparent, the dialogue between infrastructures and overseers becomes more concrete and the minimum requirements can be more easily adapted to different profiles (SIPS, etc.).



Source: BCE - Cyber Resilience Oversight Expectation, page 7
https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf

As in the CPMI Guidance, three levels of maturity are defined incrementally, i.e. reaching a higher level requires meeting all criteria of the lower levels. Because cyber threats evolve constantly, the requirements are based on the principle of continuous improvement: at the Evolving level, institutions must demonstrate that their tools and organisation are adapted to managing cyber security risk, in accordance with a framework set by the board of directors; at the Advancing level, risk management must have the appropriate tools and be integrated into the business lines, enabling it to be proactive with regard to threats; lastly, at the Innovating level, the infrastructure is recognised for its ability to instil and share best practices with its various stakeholders, for the benefit of the entire financial sector ecosystem.

Structured on the basis of the same risk management categories as the NIST framework[2] and the CPMI Guidance, the requirements are grouped by section according to a model illustrated by the following diagram:

Each section begins with an overview directly inspired by the CPMI Guidance that provides an understanding of the scope and intent of the requirements. This segmentation into eight sections clearly highlights the strengths and avenues for improvement of the infrastructure being assessed, leading to a more direct dialogue with the overseer. Nevertheless, a global approach, in which each area interacts with the others, must be adopted to reach the required level.

This initial version of the framework was applied in 2020 to several systemically important payment systems. The initial feedback on the four systemically important European payment systems (assessments carried out in 2020) is positive, in particular because it is part of a short, medium and long-term improvement process. Other infrastructures will be assessed gradually, in the spirit that guided the creation of this framework: transparency and clarity of overseers' expectations, as well as improving the resilience of the entire European financial sector.

1 Governance, Identification, Protection, Detection, Response and recovery, Testing, Situational awareness, Learning and evolving

2 NIST Framework for Improving Critical Infrastructure Cybersecurity

❺ The Commission's legislative proposal on digital resilience (Digital Operational Resilience Act – "DORA")

After a public consultation phase in early 2020, on 24 September 2020 the European Commission published a set of legislative proposals aimed at promoting the digital transformation of the financial sector, including the draft European DORA regulation. This regulation is the "security" aspect of this initiative, in effect showing that cyber risk has become systemically important for the financial sector.

DORA defines a common legislative base that applies to virtually the entire financial sector, understood broadly. Therefore, it covers a wide variety of entities, both in terms of activity and size: credit institutions, payment institutions, electronic money institutions, investment firms, digital asset service providers, CCPs, CSDs, trading venues/regulated markets, trade repositories, insurance and reinsurance companies (and intermediaries), pension funds, rating agencies, statutory auditors, benchmark rate administrators and crowdfunders.

Specifically, DORA aims to achieve "top down" harmonisation of all existing provisions that currently appear in a large number of sector-specific laws (directives and regulations), which are generally organised in silos specific to each category of player. The regulation would be directly applicable, and focuses on four major issues: (i) IT governance and risk management requirements, (ii) security incident reporting, (iii) security testing, and (iv) third-party IT risk management. It also includes considerations on information exchange and cooperation between authorities. This harmonisation should eliminate differences and redundancies between sector-specific regulations, which lead to competitive distortions and regulatory arbitrage.

DORA is consistent with the principle of proportionality. Firstly, there will be exemptions from IT risk management requirements for micro-enterprises and, secondly, certain obligations, such as conducting advanced tests, will only apply to entities deemed systemically important.

Lastly, the management of risks associated with IT providers ("third-party IT risk") is the real institutional innovation of this regulation, in particular, the introduction of direct oversight by the authorities of a selection of providers identified as particularly important for the financial sector. However, each financial institution will be fully responsible for its compliance with DORA, even if it outsources certain services to IT providers.

❻ Best practices for CCP auctions

Because counterparty risk management is essential for CCPs, dealing with the possible default of a clearing member is a core component of their business. If a default occurs, the CCP must redistribute the defaulting member's portfolios in a very short time (a few hours or days). To do so, it may either liquidate these positions directly on the market or auction them off to other members (default management auction). At the conclusion of this process the CCP will be able to determine the final loss due to the member's default, which it will absorb through the default waterfall (the margins of the defaulting member, then a share of the CCP's capital (skin in the game), then the mutualised default fund). Therefore, reasonable (i.e. sufficiently high) bids from members for the portfolio in default ultimately limit the losses absorbed by all members.

In September 2018, the Swedish CCP Nasdaq Clearing's management of the default of an individual trader led to the default fund absorbing significant losses (over EUR 100 million). In particular, the CCP's auction of the member's positions was criticised, which reaffirmed the value of the CPMI-IOSCO's work on this issue that began in early 2018.

This led to the creation of a project to identify the practices of CCPs with respect to auctions, in particular the operational challenges thereof, to establish common definitions and to describe the expected points to be monitored. This project was carried out in close collaboration with the industry, in particular through workshops and questionnaires, and concluded with the publication in June 2019 of a consultation document[1] and then, taking into account the reactions thereto, a final public report in June 2020.[2]

The report first describes governance expectations, with the need for clear delegations from the board of directors and the utility of default management groups (DMGs) comprising external participants. To increase the likelihood of a successful auction, the CCP must define its portfolio hedging strategy in advance in order to reduce the associated risk and therefore make the portfolio more attractive to buyers. It may also split the portfolio into several segments to make them easier to absorb. The various auction formats are described (Dutch, single unit pay your price, two-way pricing, etc.), along with their respective advantages in terms of confidentiality or the potential for receiving the best bids. Emphasis is placed on the importance of having a broad base of auction participants and incentives are suggested that can be used for this purpose (e.g. mandatory participation, "subordinating" the contributions to the default fund of the least cooperative members). The CCP must conduct frequent "fire drills" to test the entire operational process. Since the COVID-19 crisis emerged in March 2020, the European authorities have also particularly verified the ability of the CCPs to manage a default remotely.

The CPMI-IOSCO identifies several points on which industry progress is expected within two years: i) standardisation of auction terminology and files; ii) involvement of clearing members in governance and participation of end clients in auctions, and the related conditions; and iii) coordination between various CCPs of the hedging strategies for the portfolios of the same defaulting member.

In mid-2022, the CPMI-IOSCO will assess the progress made and, if necessary, may issue guidance setting out the best practices to be followed by CCPs.

1 *A discussion paper on central counterparty default management auctions,* June 2019.

2 *Central counterparty default management auctions – Issues for consideration et Cover note to the CPMI-IOSCO report on CCP auctions,* June 2020.

7 The impact of COVID-19 on market infrastructure activities

The health crisis caused by the COVID-19 pandemic provided a test of the soundness of the financial system and the robustness of the reforms implemented following the 2008 financial crisis.

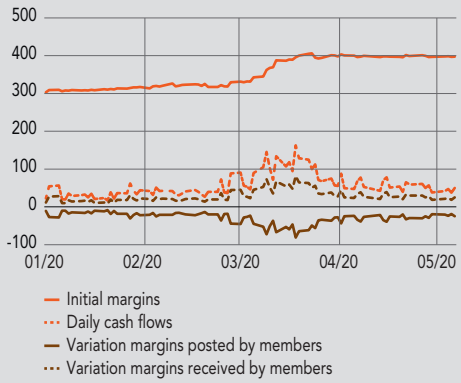
The CCPs proved resilient to market disruptions, both operationally and financially.

In mid-March, at the height of the crisis, the financial markets experienced extreme levels of volatility, resulting in (i) price movements that at times exceeded those seen in 2008, (ii) a sharp increase in daily trading volumes and (iii) a deterioration in liquidity in certain sectors (such as the equities market). The largest European CCPs showed resilience in this difficult environment and effectively managed the risks to which they were exposed. However, the sharp increase in the frequency and volume of margin calls raised more structural questions about the pro-cyclicality of CCP margins, an issue that regulators continue to monitor closely.

Following the general trend, the volumes that LCH SA cleared in March increased in all its business segments. In particular, the EquityClear and CDSClear segments experienced volumes between two and three times higher than normal trading volumes. The initial margins called by the CCP increased by around 35%. Nevertheless, LCH SA demonstrated robust crisis management and all clearing members continued to fulfil their obligations to the CCP.

From an operational point of view, one of the particularities of this crisis has been the widespread use of teleworking, which has impacted all financial market players. The unavailability of the CCPs' work sites required them to be able to continue to operate effectively remotely, which resulted in

C1 Initial margins and variation margins posted to the four largest European and UK CCPs
(in EUR billions)



Source: ESRB Report, June 2020.

the implementation of contingency plans and crisis management units, a switch of over 90% of their staff to remote working and the strengthening of IT and communication systems, as well as cyber protection systems.

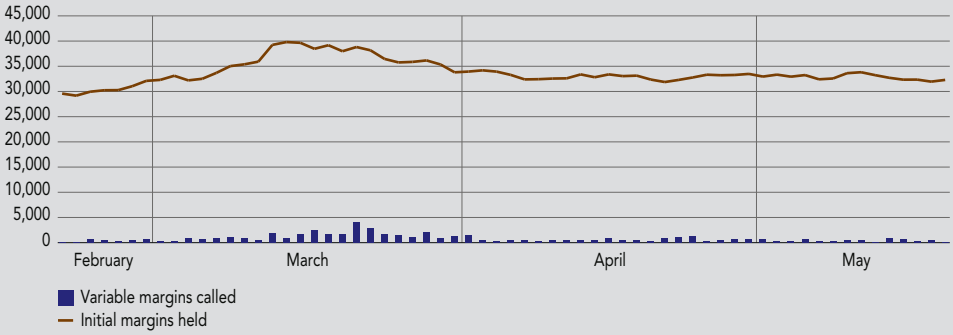
At the same time, the competent authorities paid particular attention to the mechanisms and procedures for managing defaults. LCH SA has accordingly carried out several fire drills since the start of the crisis, which have proved the CCP's operational capacity to remotely manage the possibility of default by clearing members.

Central securities depositories successfully implemented their continuity plans in response to the COVID-19 health crisis, and effectively dealt with the sharp rise in volumes

On 16 March 2020, Euroclear France imposed teleworking on over 90% of its staff, with a very limited physical presence (only for certain functions, in particular IT).

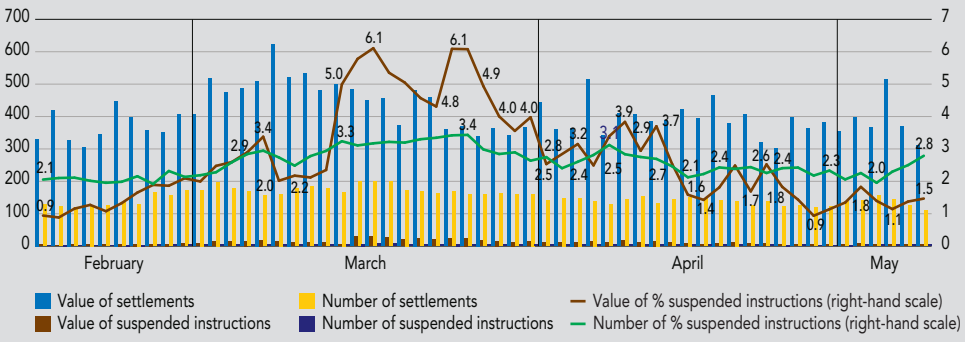
During the first weeks of the COVID-19 crisis, Euroclear France experienced a sharp increase in the volume and value of transactions, and its processing capacity enabled it to absorb these very high volumes. This increase in volumes and the impact of the constraints associated with the lockdown of back office teams resulted in significantly higher suspense rates, which impacted all Euroclear France participants. Transaction volumes and suspense rates subsequently stabilised in mid-April.

C2 Change in LCH SA's initial margins and variation margins (in EUR millions)



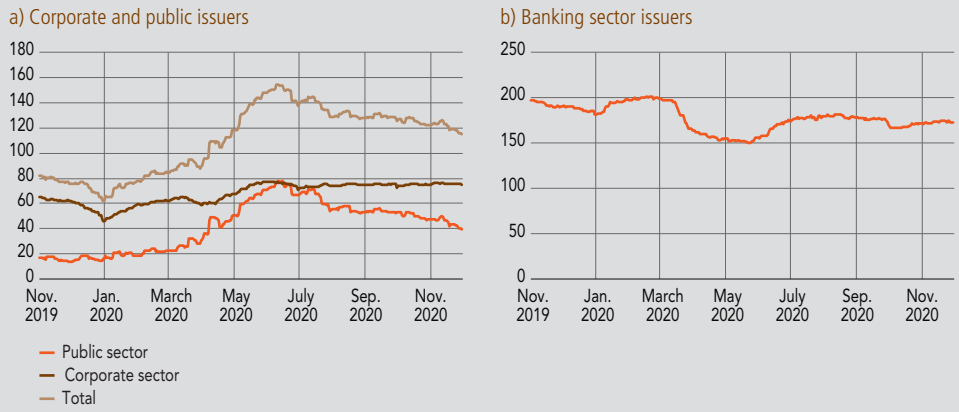
Source: 2020 market and risk mapping, AMF, July 2020.

C3 Change in Euroclear France's activity during the crisis (right-hand scale,%)



Source: 2020 market and risk mapping, AMF, July 2020.

C4 NEU CP outstanding amounts (billions euros)



Note: Les NEU CP – *Negotiable EUropean Commercial Paper* – sont des titres négociables à court terme.
Source: Banque de France.

ID2S switched its entire staff to full teleworking on 16 March 2020. The continuity plan was implemented without operational difficulties. When lockdown was lifted, teleworking continued to be encouraged as only 50% of the workforce could be present on site at the same time. When the second lockdown was announced, ID2S switched all of its staff back to teleworking.

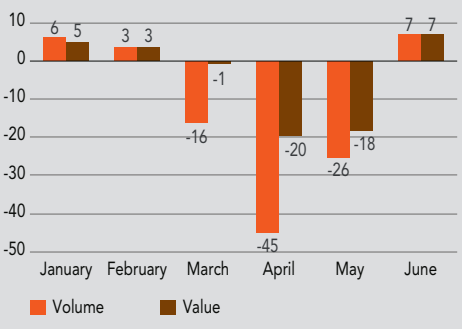
The upswing in the NEU CP market since May 2020 is mainly due to corporate issuers and issuers of social security debt (including *Caisse d'amortissement de la dette sociale* (Social Security Debt Repayment Fund)).

French payment systems proved efficient and resilient in the first wave of the COVID-19 pandemic

At the operational level, STET updated its business continuity plan (BCP) in February to incorporate COVID-19-related scenarios. It introduced teleworking at scale in mid-March and continued to manage its activities effectively remotely.

The monitoring of its activity detected no incidents or delays. In terms of flows, it noted a decrease in payment volumes and values against a backdrop of an overall decline in economic activity and consumption. The first lockdown, from 17 March 2020 to 11 May 2020, impacted payment instruments differently. Payments that require a specific action by the payer (cards, ATM withdrawals, cheques) experienced the biggest drop in use. In April 2020, card use fell by 49% in volume and 40% in value (despite the increase in the share of e-commerce compared with traditional shops), before posting an increase in volume and value in June 2020 relative to June 2019.

C5 Impact of lockdown on flows exchanged via CORE(FR)
Variation in volumes and average values settled between 2019 and 2020 (%)



Source: STET, authors calculations.

2

OVERSIGHT OF CASHLESS MEANS OF PAYMENT BETWEEN 2018 AND 2020

OVERSIGHT OF CASHLESS MEANS OF PAYMENT BETWEEN 2018 AND 2020

1 Regulatory changes in the field of cashless means of payment

1.1 Finalisation of the regulatory package in connection with the second European Payment Services Directive (PSD2)

After the introduction of the euro as a currency in 2002 and the introduction of SEPA means of payment in 2014, the integration of the European payments market continued through regulatory channels. The first European Payment Services Directive ("PSD1") and the two European directives on electronic money ("EMD1" and "EMD2"), which were adopted in the 2000s, had already laid the foundations for a harmonised regulatory framework for payment services in Europe. The aim was both to provide added consumer protection and establish a competitive and innovative market. In particular, since their entry into force, two new categories of financial institutions, payment institutions (PIs) and electronic money institutions (EMIs), have been authorised to provide payment services alongside banks. By 2020, the *Autorité de contrôle prudentiel et de résolution* (ACPR) had authorised 58 active institutions as PIs or EMEs, after obtaining the opinion of the Banque de France on the security of the payment services offered.

The second European Payment Services Directive ("PSD2"), which was adopted on 25 November 2015, extended the scope of European regulations to two new payment services: account information services and payment initiation services. The particularity of these two new payment services is that they are dissociated from keeping a payment account or directly handling the customer's funds. However, they allow authorised payment service providers (PSPs) to access and perform transactions on accounts opened at another institution, at the customer's request. PSD2 also introduces strong customer authentication requirements for in-person or remote electronic payments and for all sensitive transactions at risk of fraud.

PSD2 was transposed into French law in 2017 and came into force in January 2018, with the exception of the security requirements of the delegated Regulation (EU) No. 2018/389 on regulatory technical standards for strong customer authentication (SCA) and secure open standards of communication (CSC) (known as "RTS on SCA and CSC"), which came into force 18 months later in September 2019. This RTS SCA & CSC regulation governs access to payment accounts by third-party providers (TPP) authorised to provide account information and payment initiation services. In particular, it specifies the security rules for application programming interfaces ("APIs"), which are created by the institutions that hold the accounts specifically for access by third-party providers. The RTS Security regulation also sets out the requirements and exemptions for strong customer authentication for electronic payment transactions and sensitive transactions.

Several European Banking Authority (EBA) guidelines have supplemented PSD2 and specify the conditions for its application, including with respect to security-related issues for which the Banque de France is the competent authority in France:

- As required by the directive, the EBA adopted three guidelines that specify the obligations of payment service providers with respect to managing operational and security risks (EBA/GL/2017/19),[1] notifying major incidents (EBA/GL/2017/11)[2] and reporting fraud data (EBA/GL/2018/05).[3]

1 In 2019, these guidelines were incorporated into the Guidelines on ICT and security risk management (EBA/GL/2019/04).

2 These guidelines are in the process of revision through a public consultation launched on 14 October 2020.

3 These guidelines were amended by new guidance in 2020 (EBA/GL/2020/01), which provided some additional clarifications.

- The EBA has also produced guidelines specifying the conditions to exempt account servicing payment service providers that have opted for a dedicated interface from the obligation to set up the contingency mechanism described in Article 33(4) of the RTS on SCA & CSC (EBA/GL/2018/07), as well as four opinions on the implementation of RTS on SCA & CSC (EBA-Op-2018-5), the use of eIDAS certificates (EBA-Op-2018-7), the elements of strong authentication (EBA-Op-2019-06) and obstacles to the provision of account information and payment initiation services (EBA-Op-2020-10). The latter document identifies practices of institutions managing accounts that may create operational obstacles to the ability of third-party providers to provide their services.

Finally, questions regarding the implementation and interpretation of the PSD2 regulatory package may be submitted to the EBA, the answers to which are prepared in conjunction with the European Commission, as well as national competent authorities such as the Banque de France and the *Autorité de contrôle prudentiel et de résolution* (ACPR). As at 31 August 2020, the EBA had published 118 responses to questions on the application of PSD2.[4]

1.2 Incorporation of PSD2 into the Banque de France's oversight system

Firstly, PSD2 imposes new requirements on collecting statistical data on means of payment use and fraud. Starting in 2021, the EBA's requirements for reporting fraud-related data (EBA/GL/2018/05) will be incorporated into the Banque de France's "*Means of payment mapping*" and "*Report on means of payment fraud*", which will become half-yearly. All payment service providers (PSPs) established in France are subject to these statistical collection requirements. The schedules, completion guides and submission procedures are available on the Banque de France website.[5]

In addition, the template for the annex to the internal control report on means of payment security, which is required by Article 262 of the Order of 3 November 2014 on the internal control of financial institutions, was amended in 2019 to cover issues around secure access to payment accounts and their information and to include the audit report to be prepared by the PSPs on the implementation of RTS on SCA and CSC. This template is available on the website of the *Autorité de contrôle prudentiel et de résolution* (ACPR).

Finally, under the laws transposing PSD2, PSPs are required to notify the Banque de France of the occurrence of the following events:

- the blocking of access by a third-party PSP due to unauthorised or fraudulent access;[6]
- the failure to immediately reimburse an unauthorised payment transaction if the PSP suspects user fraud;[7]
- major security incidents.[8]

1.3 The OSMP migration plan for strong authentication on online payments

The PSD2 security requirements aim to ensure a high level of security for online electronic payments through the widespread use of strong payer authentication. These security measures came into force on 14 September 2019. However, due to the timeline required to upgrade protocols and systems by both banks and merchants, the OSMP has defined a migration plan for the French market, in accordance with the European Banking Authority's opinion of 16 October 2019 (EBA-Op-2019-11). This migration plan grants market participants additional time, until 31 December 2020, to comply with strong customer authentication requirements for online card payments. This migration plan has two aspects:

- An aspect aimed at consumers that focuses on enrolling cardholders in authentication systems that meet the PSD2 definition of strong authentication, replacing the use of One Time Password SMS (or OTP SMS) as a sole authentication factor.
- An aspect aimed at professionals in the payments ecosystem, including e-merchants, that focuses on developing authentication infrastructures, particularly the 3-D Secure technical protocol, to ensure application of PSD2's strong authentication liability and exemption rules.

Monitoring indicators with targets and deadlines, as well as action plans, have been developed for these two aspects to facilitate compliance by the French industry. However, the health crisis-related lockdown which ran from mid-March to mid-May 2020 impacted the initial migration plan. In response, the plan was adjusted in 2020 to include additional flexibility. At the same time, the Observatory adopted a number of additional measures in order to achieve the highest level of compliance within the deadlines set by the European Banking Authority:[9]

- Firstly, the Observatory ensured that version 2 of the 3-D Secure protocol was fully available to e-merchants.
- It then defined a soft decline deployment plan for the

French market, from September 2020 to March 2021. This mechanism enables card issuers to reject a transaction that does not comply with PSD2 while allowing e-merchants to resubmit the transaction via 3-D Secure.

- Lastly, the Observatory ensures the resilience and appropriate quality of infrastructures used to implement strong authentication requirements when they are in general use. A mechanism for processing payment flows in the event of a failure of these infrastructures must be defined to ensure that, within a standardised common framework, incidents are detected, information is shared at market level and alternative processing methods are activated.

1.4 Roll-out of dedicated interfaces used to access payment accounts

The second security component of PSD2 concerns the conditions for accessing payment accounts by third-party service providers authorised to provide account information and payment initiation services (hereinafter, "third-party providers"). Although PSD2 contributes to opening banking platforms ("Open Banking"), it also seeks to preserve the security of banking data and transactions. Since the RTS on SCA & CSC came into force on 14 September 2019, institutions that manage accounts are required to allow access to their customers' payment accounts by authorised third-party providers at no charge. Three access methods are possible to meet this requirement:

- Providing access via the usual online banking interface, with authentication by the third-party provider (i.e. without a dedicated interface);
- Providing a dedicated interface (API) with contingency mechanism, generally based on the online banking interface, with authentication by the third-party provider;
- Providing a dedicated interface (API) without a contingency mechanism, after the ACPR has granted an exemption from the requirement to provide a contingency mechanism (see section 2.7).

The regulation thus aims to put an end to the practice of unauthenticated web scraping by third-party players. This practice consists in using the customer's personalised security credentials, i.e. their bank login and password, to access their payment account and data. This generates two risks. Firstly, it does not allow the institution that manages the account to identify connections by third parties. Moreover, it obliges customers to share sensitive data, which ordinarily should remain strictly confidential.

In order to support a community-defined dedicated interface model (API), in April 2018 the Banque de France and the ACPR created a working group on APIs favoured by PSD2, under the auspices of the *Comité National des Paiements Scripturaux* ("CNPS" - National Cashless Payments Committee). The role of this working group was (i) to identify and resolve sticking points hindering the deployment and use of dedicated interfaces, (ii) to relay and explain the clarifications made at European level and (iii) to share statistical indicators on the use of APIs. Ultimately, by the end of 2020, the use of dedicated interfaces to provide account information and payment initiation services had increased significantly. However, additional improvements are anticipated in 2021, which should further increase the rate of API use and significantly reduce the practice of unauthenticated web scraping.

1.5 New recommendations issued by the OSMP

Security monitoring is a key component of the oversight of means of payment: it aims to identify the risks associated with the development of new payment solutions, new technologies or new fraud techniques, and then to determine the measures that can prevent these risks from materialising. As a general rule, this monitoring is carried out in cooperation with market participants through a permanent working group of the OSMP, which results in recommendations published in the Observatory's annual reports. The monitoring work carried out in this respect focused in particular on:

- The security of SEPA payment methods (OSMP 2017 annual report): this study analysed the operation of SEPA credit transfers and direct debits and identified the security measures appropriate to the various types of uses thereof. The Observatory's recommendations focused on developing enhanced authentication of transactions in accordance with PSD2 requirements, developing tools to assess the level of risk of transactions, and securing sensitive payment data throughout the payment chain.

4 The answers can be found on the European Banking Authority's website via the following link: *https://eba.europa.eu/single-rule-book-qa*

5 Via the following link: *www.banque-france.fr/stabilite-financiere/securite-des-moyens-de-paiement-scripturaux*

6 At the following address: *2323-NOTIFICATIONS-UT@banque-france.fr*

7 Via a monthly statistical collection to be submitted through the ONEGATE-OSCAMPS collection portal.

8 Via a dedicated secure interface, the access procedures for which are provided on request via *2323-NOTIFICATIONS-UT@banque-france.fr*

9 Details of these measures are set out in the 2019 annual report of the OSMP.

- The security of non-connected payment methods (2018 annual report), i.e. cheques, bank transfers ordered on paper forms and card payments communicated in paper format or by e-mail or telephone (known as mail order/telephone order (MOTO) transactions): this study analysed the specific risks associated with these lingering practices and highlighted the methods and parameters that increase their security. The Observatory's recommendations are particularly intended to reduce weaknesses due to the absence of strong payer authentication and, therefore, focus on implementing advanced systems for identifying the authenticity of transactions on initiation and high-risk transactions when they are processed. Pursuant to the national payments strategy promoted by the *Comité national des paiements scripturaux* (CNPS), the Observatory also encourages the development of alternative solutions to these practices that are intrinsically more innovative and secure.

- Mobile payment security (2018 annual report): this study provided an overview and described the latest developments in mobile payment solutions, with particular focus on techniques for processing sensitive payment data used by these solutions, such as tokenisation. The Observatory's recommendations concern the protection of sensitive payment data by all players involved, developing enhanced authentication, particularly with regard to the registration of cards in mobile payment applications, implementing risk analysis tools and setting up a protective contractual framework for users of mobile payment solutions.

- Payment data security (2019 annual report): this study analysed new risks to the security of payment data and identified best practices to ensure data protection throughout the processing chain, among users, payees and payment industry players. The Observatory's recommendations discuss effective implementation, in accordance with PSD2 requirements, of strong user authentication for access to payment services and all sensitive data, as well as support for sensitive data protection techniques, such as encryption and tokenisation, and provide a reminder to users of the prudence and confidentiality principles applicable to data.

1.6 Crypto-assets and stablecoins: new means of exchange that require changes to the payment oversight regulatory framework

Alongside traditional means of payment, the creation of bitcoin in 2008 gave rise to a new category of assets, crypto-assets, which can be used as means of exchange. These assets combine two innovative technologies that make it possible to secure transactions, including in the absence of a trusted third party: (i) blockchain, which irreversibly links transactions, and (ii) distributed ledger technology (DLT), which enables each network participant to access the history of all transactions. The use of these assets is still very limited in connection with transactions, but the rise in their value has sparked media interest, attracted certain investors for speculative purposes and led to the emergence of a new entrepreneurial ecosystem.

Although these assets are innovative, their use nonetheless entails risks that have become clearer with experience: in addition to the possible loss of capital due to their volatility, the anonymous nature of exchanges makes them conducive to illicit transactions (money laundering, terrorist financing and tax evasion). Moreover, in the absence of legal protection, users are particularly vulnerable to scams and cyber attacks.

Various jurisdictions have responded in disparate fashion to the emergence of these assets, which do not fit into any pre-existing legal frameworks. Whereas some countries have attempted to prohibit all crypto-asset activities or to incorporate them into existing legal frameworks, such as financial instruments, other jurisdictions, such as France, have opted for an ad hoc legal framework: in 2018, the PACTE Law created a new status of digital asset service provider (DASP). Service providers that provide custody or purchase/sale services for digital assets in legal tender are required to register as a DASP with the AMF. Before deciding on the outcome of any application, the AMF requests the ACPR's confirmation of compliance with anti-money laundering and counter-terrorist financing laws. For other digital asset services recognised by the PACTE Law, approval by the AMF is optional. However, in view of the naturally international nature of these activities, convergence – or at least some form of close cooperation – between jurisdictions is necessary. In 2014, the Financial Action Task Force (FATF) conducted a study of the money laundering and terrorist financing risks associated with crypto assets,[10] and subsequently modified its recommendations in 2019 to provide a specific framework for these assets.

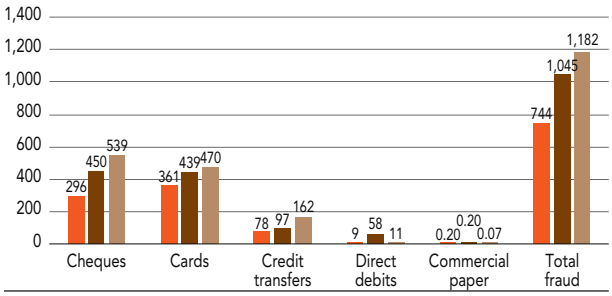
Questions about the nature of these assets and the related role of central banks took on a new dimension following Facebook's announcement of the Libra project in 2018. This event was greeted with caution given the growing influence of technology companies (or BigTechs) in the payments industry, but especially due to its potentially disruptive effect. According to its developers, Libra would be able to overcome the main limitation of first-generation crypto-assets, namely their unstable valuation, by indexing

valuation to a basket of currencies that are legal tender – hence the term stablecoin. Unlike decentralised crypto-assets, Libra would be issued by a central entity, which would be responsible for its indexation. The network also aims to bypass traditional payment infrastructures in order to overcome certain deficiencies, particularly in the area of cross-border payments.

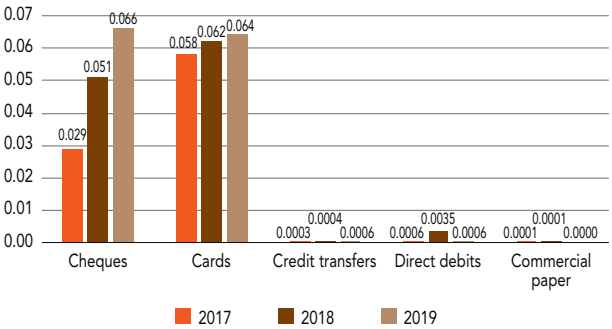
In light of this challenge, the G7 analysed the potential impact of the emergence of global stablecoin networks. Its report, which was published in October 2019 under the French presidency, highlights the risks generated (in particular, in terms of financial stability, customer protection and compliance with AML-CTF provisions) and calls for a coordinated international response before any stablecoin is launched. At the same time, the FSB undertook work on this issue, which led to the publication, in October 2020, of a report proposing both regulatory and supervisory adjustments. In a similar vein, in September 2020 the European Commission published a draft European regulation dealing with crypto-assets, known as Markets in Crypto-assets (MiCA).

C5 Means of paiement fraud from 2017 to 2019

a) Means of paiement fraud (in millions of euros)



b) Means of payment fraud rates (%)



Source: Banque de France, Observatoire de la sécurité des moyens de paiement.

2 Review of the oversight of cashless means of payment

2.1 Three-year review of trends in means of payment fraud[11]

From 2016 to 2019, a period of rapid growth in payment flows, fraud involving cashless means of payment grew continuously, although the trends varied from one payment instrument to another, as discussed below:

- **Cheques** are the means of payment that were the hardest hit by fraud over this period. Since 2018, they have been the means of payment that has experienced the highest rate of fraud, despite the fact that cheque use has steadily decreased: cheque issuance has fallen by nearly 2.5 times since 2004, with 1.6 billion cheques issued in 2019 (compared to 1.9 billion in 2017, i.e. a decrease of 18% over this period). The share of cheques in the overall amount of cashless payments fraud steadily increased to 46% in 2019, with a fraud rate of 0.066%, higher than that of cards, despite the fact that cheques are used much less frequently: only 6% of cashless transactions are made by cheque, compared with 60% by card.

- If payment and withdrawal transactions are combined, **cards** have also experienced a continuous increase in fraud rates, which nevertheless remain in line with the constant increase in their use, as they account for more than half of cashless payments (60% in 2019 compared with 58% in 2017). As a result, the fraud rate for cards remained relatively stable in 2019 at 0.064% (compared with 0.058% in 2017). At national level, fraud increased only very slightly over the period between 2017 and 2019 (0.040% in 2019, compared with 0.037% in 2017). Depending on the types of transaction carried out in France, the rates of fraud for point-of-sale payments (0.010% in 2019), contactless payments (0.019% in 2019) and ATM withdrawals (0.028% in 2019) changed little over the period between 2017 and 2019. Fraud is much higher for remote payments, although the fraud rate has been falling steadily since 2012 and stood at 0.170% in 2019 (compared with 0.190% in 2017). International transactions[12] continue to be exposed to higher rates of fraud, with a fraud rate nearly seven times higher than

10 "Virtual Currencies: Key Definitions and Potential AML/CTF Risks", FATF, 2014

11 Detailed annual data on means of payment fraud are available in the annual reports of the OSMP, which can be accessed via the following link: *https://www.banque-france.fr/en/liste-chronologique/annual-activity-report*

12 Transactions carried out by French cardholders abroad and by foreign cardholders in France.

that for domestic transactions, but this situation also improved over the period (0.262% in 2019 compared with 0.281% in 2017). Fraud in international transactions has two main characteristics: firstly, it is concentrated on remote payments, which account for over 80% of fraud amounts and, secondly, it continues to be better controlled within Europe's SEPA area than elsewhere due to the gradual strengthening of European payment security laws (implementation of PSD2).

- **Credit transfers** saw an increase in fraud between 2017 and 2019, but with no impact on the fraud rate, which remains extremely low (0.0006% in 2019), due to the continued growth in payment flows and the weight in value of large transfers (which account for 46% of the amounts exchanged by credit transfer in 2019). This increase in fraud is primarily the result of an increase in forged transfer orders initiated by fraudsters who usurp personal data to log on to the online or mobile banking spaces of legitimate customers. In 2019, this transaction initiation channel alone accounted for 55% of total credit transfer fraud, for a fraud rate of 0.0023% – four times higher than that for this means of payment overall.

- Among the payment instruments accessible to individuals, **direct debits** are the means of payment with the lowest annual amounts of fraud, with extremely low fraud rates over the period between 2017 and 2019 (0.0006% in 2019). Direct debit fraud is almost exclusively domestic (96% of total fraud in 2019), despite the European nature of the SEPA direct debit.

- **Commercial paper** (bills of exchange and promissory notes) remains relatively unaffected by fraud, with the lowest fraud rates over the period between 2017 and 2019.

2.2 Security evaluation at the time payment and electronic money institutions are authorised

The ACPR consults the Banque de France on the technical, IT and organisational resources in relation to payment instrument security when reviewing authorisation applications, in accordance with Article L. 141-4 of the *Code monétaire et financier*. The Banque de France issues an opinion in response to these consultations. Between 1 January 2018 and 30 September 2020, the Banque de France prepared and provided 70 positive opinions to the ACPR, in certain cases subject to conditions precedent, on:

- 40 authorisation procedures for payment institutions or electronic money institutions and registration procedures for account information service providers.

- 12 authorisation extension procedures for the provision of other payment services by payment institutions or electronic money institutions.

- 18 payment institution or electronic money institution exemption procedures on the grounds of the limited range of goods and services that can be acquired using the means of payment offered or the limited network of entities that accept them.

With the exception of institutions exempt from authorisation, these institutions are subject to Banque de France oversight, as are all payment service providers (PSPs) that do business in France.[13] More specifically, these PSPs are subject to all fraud data reports requirements to the Banque de France, as well as the requirement to provide information on changes to their risk management systems. They may also be subject to onsite inspections.

2.3 Review of the oversight of issuers of means of payment

After the payment service provider authorisation stage, the oversight system applicable to issuers of cashless means of payment includes several types of actions:

- Records-based inspections, i.e. a review of the documents and statistical data that institutions are required to submit to the Banque de France on a periodic basis or on request;

- On-site inspections, i.e. audits of specific issues conducted on the institutions' premises and, potentially, those of their subcontractors;

- Bilateral exchanges with institutions in the form of interviews, on a regular basis or depending on current events.

Through these various oversight actions, the Banque de France assesses issuers' compliance with the various security standards issued by the Banque de France or the Eurosystem.

Review of the level of institutions' compliance with the cheque security framework

The cheque security framework (CSF) describes the security objectives of institutions involved in processing cheque transactions. It is supplemented by an assessment questionnaire specifying the procedures for implementing these security objectives. Credit institutions are required to assess their level of compliance with these objectives annually. A new version of the CSF took effect on

1 January 2017 and, therefore, institutions submitted their first assessment based during the first half of 2018. The first two years of the new framework highlighted both a satisfactory overall level of compliance and shortcomings with respect to several categories of objectives. The security objectives with the lowest level of compliance concern both the physical security and protection of cheques, their physical delivery to holders, ensuring holders' awareness of cheque-writing rules, mechanisms for monitoring transactions and, lastly, the formalisation of security in terms of governance and organisation.

These vulnerabilities should be seen in light of cheque fraud trends since 2017. Although the drop in cheque use continues (-10% on average per year), the fraud rate for this means of payment continues to rise, making it the means of payment with the highest rate of fraud over two consecutive years (2018 and 2019 data). In order to break this trend, the OSMP included specific work to combat cheque fraud in its 2019-2020 work programme. This work was carried out with all players in the cheque-processing chain with a view to proposing a set of additional actions aimed at increasing the security of the entire processing chain, as well as the vigilance of users, issuers and payees, while respecting the specific nature of the cheque's paper format.

Review of on-site audits of the quality of statistical reports

The collection of statistical data on the use of means of payment and fraud is an essential component of the Banque de France's oversight duties, which enables it to both direct its action and measure its results. For this reason, on-site audits of four banking groups were conducted in autumn 2017 to assess the compliance of data collection processes and reporting for the Banque de France's "*Means of payment mapping*" and "*Report on means of payment fraud*". The recommendations made at the end of these audits focused on two aspects:

- Firstly, shortcomings or anomalies were identified in the practices of the audited institutions with regard to the organisation, management, processes, tools, control and quality of statistical reports. Recommendations were made to the relevant institutions to be implemented via an action plan to be monitored by the Banque de France's oversight teams.

- Secondly, methodological points were identified that were open to interpretation, which led the Banque de France to refine and clarify its requirements in terms of statistical reporting vis-à-vis the reporting institutions. The points thus identified were incorporated into the Banque de France's roadmap for changes in collection of payment statistics, and also informed the European work on this issue when the EBA guidelines on fraud reporting (EBA/GL/2018/05) were negotiated and the ECB Regulation on payment statistics (ECB/2013/43) was amended.

Review of on-site audits of neobank payment security systems

The Banque de France has observed that the sometimes very rapid development of new account-holding institutions (or neobanks) could create a favourable climate for fraudsters, who in particular use this type of account as the initial destination for the proceeds of fraudulent transactions targeting other institutions before the funds are transferred abroad. The high frequency of alerts on this issue prompted on-site audits to assess the quality of the systems implemented by the main neobanks active in the French market. These audits were conducted in 2018 at four institutions authorised as electronic money institutions or payment institutions.

They showed that the audited institutions, which have highly diverse business models and risk profiles, could further strengthen their fraud risk management and control systems. In particular, recommendations were issued in 2019 for these institutions focusing on:

- Improving the structure of their internal fraud prevention systems by enhancing their statistical identification process for cases of fraud and by imposing their security requirements on their service providers and agents;

- Improving their KYC processes and developing more sophisticated monitoring tools to better detect and prevent fraudulent transactions;

- Undertaking significant upgrade projects (strong authentication solutions at the time of issue, compatibility of infrastructures with version 2 of the 3-D Secure protocol) to comply with the new strong authentication measures required by PSD2.

13 See 2014 Oversight Report – Section 4.1.2

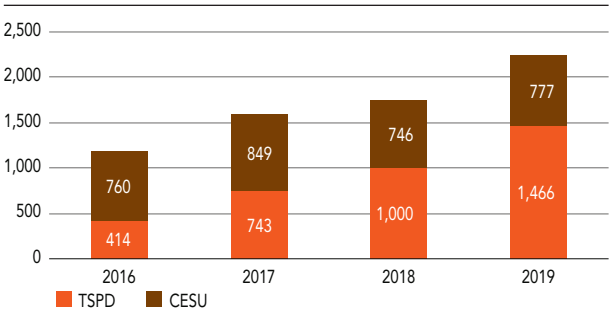
2.4 Review of oversight of special paperless payment orders and universal employment vouchers

In addition to its oversight of the security of traditional means of payment, since the adoption of Law No. 2013-100 of 28 January 2013, the Banque de France has also been responsible for the security of special paperless payment orders (*titres spéciaux de paiement dématérialisés*, hereinafter "TSPD") and the pertinence of the security principles applicable in this area. The list of TSPDs was established by the Order of 17 June 2013 and includes primarily pre-paid universal employment vouchers (*Chèque Emploi-Service Universel*, hereinafter "CESU"), which are employment cheques used by individuals to employ someone for casual labour and part-time domestic help, as well as meal vouchers, holiday vouchers, entertainment vouchers and gift vouchers. These TSPD oversight duties complement the Banque de France's oversight of paper-format universal employment vouchers pursuant to Articles R. 1271-10 and R. 1271-15 of the Code du travail (Labour Code): these provisions stipulate that, after obtaining the consent of the Banque de France, CESU issuers are authorised and undertake to comply with the security objectives that it defines.

The Banque de France's oversight system is based on the security standards for universal employment vouchers and special paperless payment orders, both of which were published in 2015. Concretely, this oversight takes the form of a self-assessment questionnaire on compliance with the Banque de France's standards that is submitted every three years by issuers, as well as operational fraud statistics collected from the same issuers. Bilateral interviews are also conducted with the main issuers of TSPDs and CESUs.

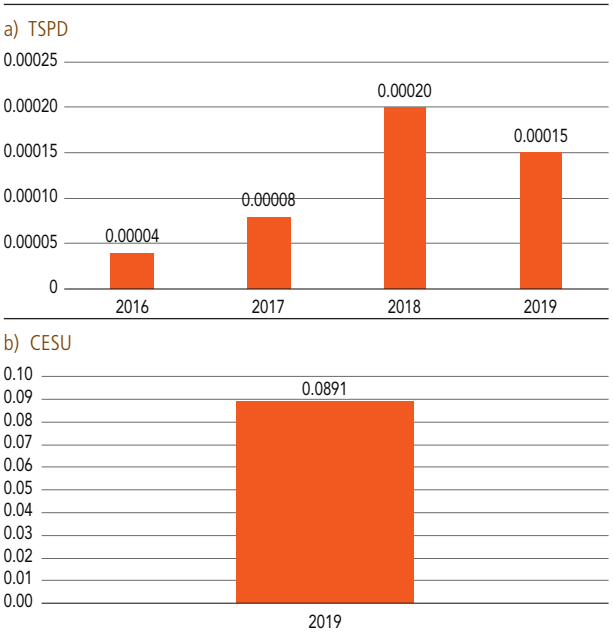
The level of compliance with the security standards for TSPDs and CESUs is satisfactory overall, but a very significant fraud event involving paper-format CESUs led to a spike in the CESU fraud rate in 2019 (0.09%, i.e. a fraud rate higher than for cheques and cards). The fraud rate for TSPDs, by contrast, remains extremely low. Overall, total TSPD and CESU fraud amounted to EUR 695,000 in 2019. However, the methodology used by certain issuers to identify fraud is unclear. For example, when meal vouchers in the form of cards are lost or stolen, some holders simply block their cards without contesting unauthorised transactions, which may prevent issuers from having a complete picture of the extent of fraud. However, the security of TSPDs and CESUs is being strengthened as they become increasingly paperless, which enables deploying strong authentication and real-time blocking and alert mechanisms.

C6 Amount of TSPD and CESU transactions (EUR billions)



Source: Banque de France, Observatoire de la sécurité des moyens de paiement.

G7 Fraud rate (%)



Source: Banque de France.

Although this activity remains a niche market (EUR 2.2 billion in transactions in 2019), these vouchers are becoming increasingly paperless, in particular due to the development of smart cards for meal vouchers and the arrival of new issuers, which is stimulating renewed competition. In 2019, TSPDs experienced strong growth with 143 million transactions (+49% from 2018), for a total amount of EUR 1.47 billion (+47%). The issuers surveyed confirmed that they expect the health crisis to accelerate companies' demand for paperless offers to replace paper offers. In 2021, *Agence nationale des chèques-vacances* ("ANCV" - National Holiday Vouchers Agency) is also expected to launch its first paperless offer and would thus come within the scope of TSPD oversight. On the other hand, the move to paperless formats has stalled for CESUs.

In 2019, in a relatively stable market (EUR 777 million, up 4.2%), the share of paper vouchers actually increased to 69% (compared with 54% in 2018).

In 2021, the oversight system for TSPDs and CESUs will change again. The statistical reports of TSPD and CESU issuers, which are currently in spreadsheet format and are submitted by email, will be submitted via ONEGATE-OSCAMPS , the Banque de France's data collection portal. At that time, statistics on both fraud and business activity will be collected twice a year, consistently with the oversight system for other cashless means of payment.

2.5 The Banque de France's contribution to the Eurosystem's payment schemes and instruments oversight actions

The Eurosystem oversight framework

The construction of the single euro payments area confers on national central banks joint responsibility for the security of means of payment. The Eurosystem has therefore developed oversight frameworks applicable to pan-European means of payment. In January 2008,[14] the Eurosystem developed an initial oversight framework to assess the security and effectiveness of card payment schemes. The oversight frameworks for SEPA direct debits[15] and credit transfers[16] were established in August 2009 and October 2010 respectively, with the *European Payments Council* (EPC) designated as the governance authority for SEPA instruments.

Evaluation guides for each of these three oversight frameworks have also been published to clarify the Eurosystem's expectations. These are intended for both oversight authorities and payment system governance authorities. These guides were updated in 2014 and 2015, notably by incorporating the recommendations on the security of internet payments published by the European Banking Authority (EBA) in 2014. After these updates, the Eurosystem began a new oversight exercise in 2016.

Oversight of card payment schemes

For card payment schemes, the oversight work took the form of a gap assessment that focused on assessing the new factors that had been introduced in the assessment guide updated in 2015. The final Eurosystem report published in 2018 provides an overview of the assessments of 16 card payment schemes, covering 13 national schemes and 3 international schemes that operate in the euro zone. The Banque de France participated very actively in this oversight work. It evaluated the six French schemes (the *Cartes Bancaires* interbank scheme and five private schemes: BNP Paribas Personal Finance, Cofidis, Crédit Agricole Consumer Finance, Franfinance and Oney Bank), the highest number in Europe. It also participated in the evaluation of three international schemes (Visa, MasterCard and American Express), which also have a significant presence in France.

The exercise revealed a high level of compliance by the French schemes with the requirements of the oversight framework, which was facilitated by the actions that the Banque de France carried out in 2009 to strengthen the security of internet payments. The Eurosystem's final report published in 2018[17] describes the widespread deployment of enhanced authentication solutions by most European schemes. Of the 16 European schemes assessed, 11 schemes (including 5 French schemes) fully complied with all standards of the oversight framework, whereas 5 schemes (including 1 French scheme) were deemed in overall compliance.

Nevertheless, there were areas for improvement in risk management, particularly in the areas of security, fraud and business continuity. As a result, concrete recommendations have been made. In 2020, no recommendations made to the French or international schemes for which the Banque de France had carried out or contributed to the assessment were still pending. The Banque de France continues to carry out regular oversight of the card schemes that operate in France to assess their organisational and technical developments and monitor their incidents.

Given the increasingly important role of tokenisation in the development of mobile payments, in 2019 the Eurosystem also decided to carry out an in-depth analysis focusing on the tokenisation activities of Visa Europe and MasterCard Europe. This analysis confirmed that the security levels associated with tokenisation are very high. Tokenisation consists of replacing sensitive data (such as an IBAN or a PAN) with substitute data, called a token, in the payment chain. This token is dedicated to a specific use and may be for single or recurring use. In most cases, tokenisation allows a card number (or PAN) to be stored centrally and

14 European Central Bank, Oversight framework for card payment schemes – standards, January 2008

15 European Central Bank, Oversight framework for direct debit schemes, August 2009

16 European Central Bank, Oversight framework for credit transfer schemes, October 2010

17 Eurosystem report on the gap assessment of card payment schemes against the "Oversight framework for card payment schemes – standards", European Central Bank, 2018

communicated to various stakeholders, without the token being misappropriated for another transaction or payment method. However, the growth in the use of tokenisation has increased the dependence of the entire payment chain on international card schemes.

Oversight of SEPA payment instrument schemes (SDD, SCT and SCT Inst)

Starting in 2016, the Eurosystem also conducted an oversight exercise on direct debits (SEPA Direct Debit, SDD) and SEPA credit transfers and, with respect to the latter, decided to simultaneously evaluate traditional credit transfers (SEPA Credit Transfer, SCT) and instant credit transfers (SEPA Credit Transfer Instant, SCT Inst) due to the similarities between them. These evaluations were carried out by a working group consisting of representatives of the national banks of Germany, Spain, France, Italy, Luxembourg and Slovakia, under the direction of the ECB. The conclusions were approved by the ECB's Governing Council in September 2018 and July 2019. In practice, the evaluation exercise focused on the audit of the governance authority of the SEPA schemes, the European Payments Council (EPC). The findings were quite satisfactory, but the report called on the EPC to strengthen its governance: firstly, by structuring the monitoring and management of fraud risks more effectively and, secondly, by verifying more frequently, if necessary using sampling techniques, the compliance of participants with the rules of the schemes.

2.6 Oversight of dedicated interfaces used to access payment accounts

Article 521-8 of the *Code monétaire et financier* tasked the Banque de France with ensuring the security of access to payment accounts and their information and the pertinence of the standards applicable in this area. This new competence arises from the transposition into French law of PSD2 and the opening of access to payment accounts to third-party players authorised to provide account information and payment initiation services. For this reason, the Banque de France published new security standards for payment account access interfaces in February 2019.

In accordance with Article 33 of the RTS SCA & CSC, the ACPR may, after consultation with the European Banking Authority, exempt a PSP account manager from the obligation to provide a contingency mechanism if its dedicated interface meets high levels of compliance and availability. In France, this exemption procedure falls under the joint responsibility of the ACPR, which is responsible for ensuring the interface's level of performance, and the Banque de France, which ensures its compliance with security requirements. The exemptions are formally granted by the ACPR and, therefore, the ACPR's General Secretariat acts as a one-stop shop for the institutions and specifies the procedure to be followed via an exemption request form. Under this procedure, the Banque de France provides an opinion on the security of the dedicated interface to the ACPR, which must be taken into account in the exemption decision. This opinion is based on an evaluation of the level of compliance, which must be performed by an information systems security assessment centre approved by the Agence nationale de sécurité des systèmes d'information (ANSSI - National Information Systems Security Agency). As at the end of 2020, 15 financial institutions in France were exempt from the contingency mechanism requirement applicable to APIs.[18]

The Banque de France also continuously oversees APIs dedicated to access by third-party service providers. For this purpose, since 2019, it has collected additional information via the security of means of payment annex to the annual report on internal control (RACI) that PSPs must submit annually. This annex must include the results of the audit report that the institution must prepare annually on the implementation of the RTS Security (see Article 3 of the regulation).

18 The list of institutions exempted from the contingency mechanism requirement under Article D. 133-10 of the Code monétaire et financier is available on the ACPR's website.

BOXES

❶ The FSB's work on the impact of stablecoins and the draft European MiCA regulation

In 2019, the G20 mandated the FSB to study and formulate recommendations for the stablecoin network regulatory framework, with a particular focus on global stablecoins – assets with the potential to achieve a global dimension. Further to that mandate, in October 2020 the FSB published a report entitled "Regulation, Supervision and Oversight of Global Stablecoin Arrangements". The report noted the potential value of global stablecoins in promoting financial inclusion and efficiency of payments. It also highlighted the systemic risks to financial stability that these networks could generate by partially displacing currencies that are legal tender for purposes of transactions.

With the exception of several emerging countries, the FSB noted that existing laws already cover a significant portion of the activities in relation to stablecoins, thus limiting the risks associated with their development. However, the drafters of the report did not rule out the possibility that these activities may evolve over time and so partially avoid legal obligations. Therefore, it is necessary to adapt the regulatory framework in order to cover all relevant services and infrastructures and ensure fair regulatory treatment of traditional means of payment and these new means of exchange. In conclusion, the FSB requested that global stablecoin project developers comply with all laws existing or being drafted before the effective commercial launch of these new solutions.

This objective is shared by the European Commission at European level through its proposed Markets in Crypto-assets (MiCA) regulation, which was published in September 2020 in connection with its digital finance strategy. The Commission intends for this new regulation to come into force no later than 2024, 18 months after its publication in the Official Journal of the European Communities. In addition to supervising services associated with first-generation crypto-assets, such as bitcoin, the draft regulation also provides a framework for the issue, distribution and use of stablecoins that, under this regulation, would become a specific class of crypto-assets. For this purpose, the MiCA proposal distinguishes between:

- firstly, asset-referenced tokens, which are defined as a type of crypto-asset backed on a basket of legal tender currencies, products such as commodities or other crypto-assets; and

- secondly, e-money-tokens, which are backed on a single legal tender currency, the purpose of which is to serve as a means of payment and which, therefore, by definition, are equivalent to electronic money. MiCA accordingly explicitly provides that issuers of e-money tokens must comply with the provisions of the Electronic Money Directive (EMD2).

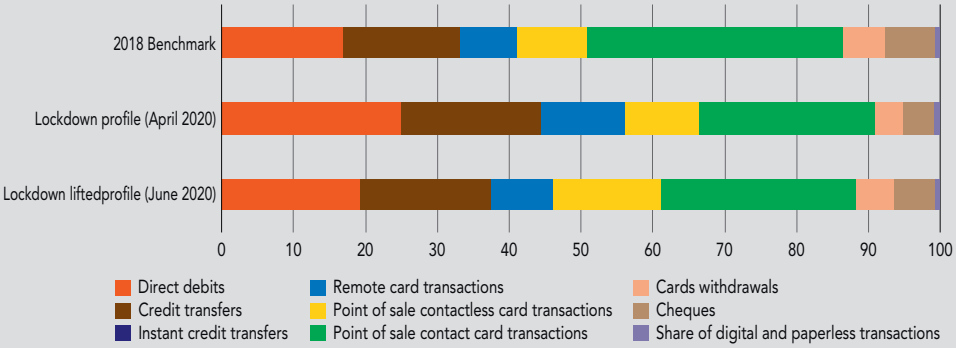
❷ Means of payment in the face of COVID-19 and lockdown measures

The French payments market proved resilient to the crisis, providing efficient and uninterrupted processing of transaction flows. However, limited difficulties were experienced with respect to two means of payment: firstly, cheques, in particular cheques over EUR 10,000 (known as "circulating" cheques), the processing of which was affected by transport problems and the temporarily reduced capacity of processing centres and, secondly, inter-company direct debits (known as "SDD B2B"), because the public authorities' announcements of reductions in certain business charges led to advance requests to cancel direct debit mandates, resulting in large numbers of rejected direct debits.

Meanwhile, the slowdown in economic activity associated with the lockdown period led to a significant decrease in payment flows. Consumer transactions were more impacted than transactions between businesses, probably reflecting a greater resilience of business and government activity relative to consumer spending. This significant drop in payment flows was accompanied by a change in payment habits: for health reasons, consumers and retailers shifted to paperless means of payment as much as possible, abandoning cash and cheques in favour of card – especially contactless – payments, mobile payments and online remote payments. Accordingly, the paperless transaction share of cashless transactions rose from 50% before the crisis to 66% in April 2020. This share fell back to 61% in June during the first weeks after lockdown, suggesting that new long-term habits may have been established during the crisis: this is for example the case of contactless cards, which had already been widely adopted by users, but which since May 2020 can be used for purchases up to EUR 50, or the even more pronounced drop in the number of cheques used in shops.

The impact of the crisis on fraud rates is still difficult to assess, as the reports on fraud statistics have not yet been submitted. However, changes in payment habits could have two contrasting effects: the displacement of cheques by cards or SEPA means of payment could have a positive impact on the overall level of fraud; conversely, the increase in remote transactions to the detriment of generally more secure in-person transactions could increase the average fraud rate for cards. However, the first indicators show a very effective containment of the fraud rate for contactless payments, despite the massive increase in their use compared with 2019 (an increase of over 50% in volume and 100% in value from July 2020).

Changes in the share of the different payment instruments in volume of transactions (%)



Source: Observatoire de la sécurité des moyens de paiement.

❸ The four pillars of means of payment security

Assessment of the security of means of payment is based on the service provider's ability to implement four complementary pillars for preventing, measuring and combating fraud.

1) Physical and logical security

The security of IT systems as a whole (systems, networks, organisation and administration of the operational activities carried out) is examined from two angles, in particular with respect to the protection of sensitive payment data: firstly, the coherence and proportionality of the physical security measures implemented for the premises and data centres, such as access controls and environmental security provisions, and, secondly, the coherence and proportionality of the logical security measures and mechanisms governing internal access to the IT systems, and specifying, for each authorised connection from the outside, the nature and frequency of the controls that the service provider will perform thereon.

2) Strong customer authentication

Payment process security covers two aspects with which the service provider complies: firstly, securing access to both account viewing and payment transactions through strong user authentication and, secondly, guaranteeing legitimate users of the payment service the availability and integrity of authentication factors, such as hardware tokens and mobile applications, both at the time of initial enrolment and on renewal.

3) Tools for detecting high-risk transactions (scoring)

The service provider must build its IT systems in a manner that makes transaction analysis possible. The goal of such analysis is to detect suspicious or unusual transactions before or after their execution. The Banque de France ensures that service providers install these detection tools and tailor them appropriately to the activity carried out.

4) User awareness

Service providers must ensure that payment service users are aware of the vigilance rules relating to the security of the payment services and tools made available to them (access rules, technical issues, keeping logins and passwords safe, etc.). The Banque de France also ensures that service providers have implemented a procedure for monitoring, processing and following up user complaints concerning security.

❹ Amendment of the ECB Regulation on payment statistics

The European Central Bank (ECB) has begun work on amending the 2013 Regulation on payment statistics (ECB/2013/43). The proposed amended regulation was the subject of a public consultation between February and May 2020 and the final version is expected by the end of 2020. This amendment is the product of an ambitious approach that seeks to adopt a single statistical framework to meet the needs of a variety of professions: in addition to oversight of means of payment, the future ECB regulation will provide for the collection of payment statistics for balance of payments and macroeconomic forecasting purposes.

With respect to the oversight of means of payment, the amended ECB regulation incorporates the statistical requirements of the European Banking Authority on means of payment fraud as set out in its 2018 guidelines (EBA/GL/2018/05). However, the ECB's proposal supplements them in several respects: firstly, by including a more detailed geographical breakdown, particularly of transactions within the SEPA; secondly, by requesting a breakdown of flows and fraud by payment scheme; and, lastly, by requesting, for cross-border card transactions, both the country of the counterparty's payment service provider and the location of the payment terminal. This new regulation is expected to come into force in 2022 and certain of its requirements will be included in the Banque de France's half-yearly "*Means of payment mapping*" and "*Report on means of payment fraud*" data collection reports.

In addition to significantly increasing the quantity and frequency of data collected from payment service providers, the draft regulation should also provide very useful data for comparing the security of means of payment at the euro zone level. Until now, the only comparative data on fraud available has been card fraud data collected from the 23 card payment systems (or card schemes) active in Europe. The sixth ECB report on card fraud was published in 2020 based on 2018 data. The trends are broadly consistent with those observed in France by the OSMP. In 2018, European card fraud totalled EUR 1.79 billion for a transaction volume of EUR 4,780 billion, i.e. a fraud rate of 0.038%. Between 2014 and 2017, this fraud rate fluctuated between 0.042% (2015) and 0.035% (2017). The slight increase in 2018, which was also observed by the OSMP, is explained by the rise in remote payment fraud (+11%) and in-person payment fraud (+3.7%), whereas the rate of fraud for withdrawals fell (-12.8%). As noted by the OSMP, remote payment fraud accounts for the vast majority of fraud (80%), followed by fraud at points of sale (15%) and ATMs (5%). It should also be noted that, international transactions are more sensitive to fraud than transactions within the SEPA and domestic transactions.

5
The future Eurosystem oversight framework for payment instruments (PISA)

The Eurosystem has decided to harmonise oversight practices by merging the existing oversight frameworks, of which there are currently five: payment instruments (2009), electronic money schemes (2003), card payment schemes (2008), direct debits (2010) and credit transfers (2010). The consultations within the Eurosystem led to a proposal for a Eurosystem oversight framework for electronic Payment Instruments, Schemes and Arrangements (PISA). The objective of this PISA framework is twofold: (i) to define a unified approach to oversight of payment solutions by applying the same principles and procedures to all solutions and (ii) to include a certain number of new services within the oversight scope, such as digital solutions and electronic wallets, referred to as "arrangements" in the PISA framework. Innovation in the payments sector has led to the emergence of new initiation methods based on a diversity of underlying payment instruments, such as mobile payment solutions based on payment cards.

The proposed PISA framework was published in October 2020 for public consultation until 31 December 2020. This project consists of three documents whose respective roles are to: (i) establish the scope and principles (Oversight framework), (ii) identify the players within the oversight scope based on their relative importance in the European payments market (Exemption policy) and (iii) specify the oversight methodology (Assessment methodology). The oversight scope would be determined on a points system based on four quantitative criteria: number of users, number of transactions by volume, number of transactions by value and geographical presence in terms of number of countries. This system should ensure that the Eurosystem's oversight work always prioritises the most important payment solutions in the euro zone. The other innovation of this PISA framework would be that it would not only cover cashless payments, but would also integrate payment solutions using assets or tokens, such as stablecoins, which are not classed as "funds" for regulatory purposes.

GLOSSARY

EBA	European Banking Authority
ESMA	European Securities and Markets Authority
CCP	Central counterparty
CFONB	*Comité français d'organisation et de normalisation bancaires* (French Banking Organisation and Standardisation Committee)
CLS	Continuous Link Settlement – US foreign exchange settlement system
CORE(FR)	A retail payment system
CPMI	Committee on Payments and Market Infrastructures
CPSS	Committee on Payment and Settlement Systems (now the CPMI)
CSD	Central securities depositories
CSDR	Central Securities Depositories Regulation – European regulation on improving securities settlement in the European Union and on central securities depositories
EMIR	European Market Infrastructure Regulation – European regulation on OTC derivatives, central counterparties and trade repositories
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 – The French securities settlement and delivery system
EURO1	A high-value payment system
FSB	Financial Stability Board
IOSCO	International Organisation of Securities Commissions
LCH SA	A central counterparty
PFMI	Principles for Financial Market Infrastructures

Rapport sur la surveillance des moyens de paiement scripturaux et des infrastructures des marchés financiers

Éditeur
Banque de France
39 rue Croix-des-Petits-Champs
75001 Paris

Directeur de la publication
Nathalie Aufauvre
Directrice générale de la Stabilité financière
et des Opérations
Banque de France

Directeur de la rédaction
Valérie Fasquelle
Directrice des Infrastructures, de l'Innovation
et des Paiements

Comité éditorial
Nicolas Péligry, adjoint à la directrice des Infrastructures, de l'Innovation et des Paiements
Pierre Bienvenu, Guillame Bruneau, Véronique Bugaj, Olivier Catau, Bernard Darrius, Florian Dintilhac, Christelle Guiheneuc, Trân Huynh, Julien Lasalle, Alexandra Madeline, Lucas Nozahic, Thomas Piveteau, Mathieu Vileyn (SMPS)
Benjamin Alford, Omar Birouk, Thomas Carré, Alexandre Garcia, Itziar Garcia Bellver, Mathieu Gex, Antoine Lhuissier, Christophe Macé, Claire Orliac, Chloé Terrier et Marie-Aline Vives (SEPI)
Alexandre Capony, Caroline Corcy, Corinne Dauchy (SEL)

Réalisation
Studio Création
Direction de la Communication

Contact
Direction des Statistiques monétaires et financières
Service d'Analyse des financements nationaux
Code courrier : 043-1418
37 rue du Louvre 75002 Paris
Courriel : 1418-CER-UT@banque-france.fr

Impression
Banque de France – SG - DISG

Dépôt légal
Janvier 2021
ISSN en cours

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

Le *Rapport sur la surveillance des moyens de paiement scripturaux et des infrastructures des marchés financiers* est en libre téléchargement sur le site Internet de la Banque de France (*www.banque-france.fr*).

www.banque-france.fr