

Current regulatory developments in the field of payments and in the settlement of securities and derivatives

The field of payments and the financial market infrastructure have evolved considerably in recent years. The Eurosystem has made substantial contributions in this regard with its TARGET2 and TARGET2-Securities payment and settlement systems, which were discussed at length in the Bundesbank's December 2017 Monthly Report. At the same time, however, regulation also has a significant impact on developments in these areas. The backdrop to this is that resilient financial market infrastructures are of major importance owing to their central functions for the financial system and the real economy. In order to ensure the secure settlement of payments as well as securities and derivatives transactions, the principles for financial market infrastructures (PFMI) were adopted by the G20 countries back in 2012. In keeping with these principles, the focus in recent years has consequently been on establishing them in a binding manner for payment systems, central securities depositories and central counterparties. The main subject of the current debate is the revision of the supervisory and regulatory framework for central counterparties that has been in place since 2012. The framework in the European Union currently being discussed envisages a stronger role for central banks and the European Securities and Markets Authority (ESMA), and, in particular, a tighter regime for the supervision of central counterparties in non-EU countries. This aspect has become particularly important in light of the forthcoming withdrawal of the United Kingdom from the European Union. In order to assess possible policy options, the Bundesbank is primarily concerned with the security of payment transactions and the settlement of securities and derivatives transactions. In addition, the recovery and resolution of central counterparties is, in future, to be harmonised throughout Europe by implementing international standards. The requirements for the monitoring of systemically important payment systems have been tightened in order, amongst other things, to counter the mounting threat of cyber crime and to give the supervising central banks new review and evaluation rights. Especially with regard to the increased threat situation, sustained efforts are needed in the area of financial market infrastructures, but also in the financial sector as a whole, to improve cyber resilience. In the EU payments landscape, the regulations are being amended significantly with the implementation of the second Payment Services Directive (PSD2), which pursues the main goal of deepening market integration within the European Union and strengthening competition. In particular, the possibility for account holders to grant third parties access to an account, which is also referred to as "open banking" in the current debate, may be a catalyst for significant structural changes in the payment services market.

Financial market infrastructures and payment services

Principles for financial market infrastructures

In response to the lessons learned from the financial crisis, regulation of the financial markets has been tightened significantly in recent years. In addition to further developing banking regulation, the rules for settling payments as well as securities and derivatives transactions were also revised and toughened. This was based on the principles for financial market infrastructures¹ (PFMI) agreed upon internationally by the G20 countries in 2012, which are also widely recognised beyond these countries. These principles formulate standardised requirements for risk management, administrative structures and the transparency of financial market infrastructures. The latter play a major role in the financial system as they are used, amongst other things, to settle financial transactions. They concentrate risks and can, owing to their central function in the closely intertwined network of the financial sector, become a major contagion channel in crisis situations. The financial market infrastructures (see the chart on page 43) include:

- Payment systems

Participants use these systems to process their payments. In some cases, payment systems are also used by other financial market infrastructures for the purpose of money settlement.

- Central securities depositories (CSDs)

Nowadays, securities are almost always held with CSDs. Investors receive the associated ownership rights via a safe custody account, which is held by the investor's bank at a CSD.

- Securities settlement systems (SSSs)

These are run by CSDs to, for example in the case of a purchase, transfer securities by

book entry from one safe custody account to another with settlement finality.

- Central counterparties (CCPs)

These entities take over the clearing – ie the transmission, reconciliation and netting as well as the risk management – of pending securities and derivatives transactions up until their maturity, interposing themselves between two trading partners. The risk positions associated with clearing are calculated by the CCP in a timely manner and on an ongoing basis and are secured by means of collateral provided by the contracting parties.

- Trade repositories (TRs)²

Trade repositories maintain a centralised and standardised record of transaction and position data for derivatives transactions.

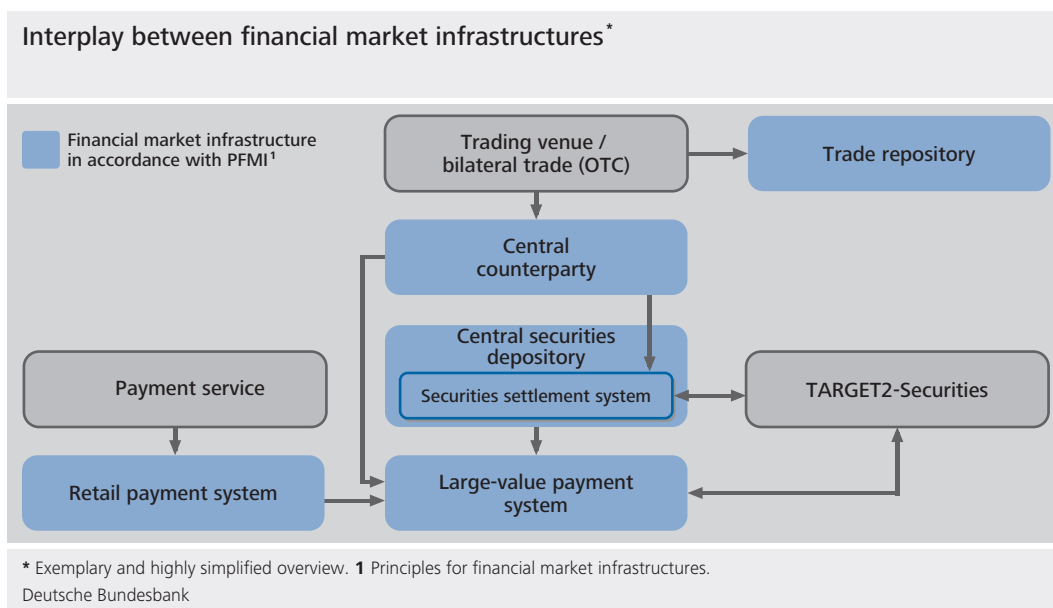
Within the EU, the PFMI have achieved a binding character for certain financial market infrastructures (eg for CCPs, CSDs and systemically important payment systems) through their consistent implementation in the shape of European legislation. The legal framework thus created is constantly being developed further in order to take account of current developments and findings.

In addition to strengthening the security and efficiency of the financial market infrastructures to protect against crises, the legal framework for the provision of payment services is also to be fundamentally revised to promote innovation and consumer rights with the aim of supporting convergence in the European single payments market.

Payment services in the single market

¹ See Deutsche Bundesbank, The new CPSS-IOSCO Principles for financial market infrastructures, Monthly Report, July 2012, pp 33-43 and <https://www.bis.org/cpmi/pub/d101a.pdf>

² The topic of trade repositories is not covered in this article.



Central counterparties

Function and significance of central counterparties

CCPs are a central component of the financial market infrastructure and serve, amongst other things, to mitigate risks in the financial system and to facilitate the settlement of transactions. As a central counterparty, they interpose themselves between the parties to financial transactions that take place at a trading venue (eg a stock exchange) or also outside trading venues (over-the-counter (OTC) transactions). A central counterparty acts as the buyer to the seller and as the seller to the buyer and thus ensures performance of the contract on behalf of both parties. CCPs therefore always have a balanced book under normal business operations, ie for each position assumed by a CCP for a market participant, there is a matching position with another market participant. In this vein, they act as risk managers for their clearing members and only to a lesser degree as risk bearers.³ In terms of risk management, the CCP uses its equity capital only to a lesser extent, instead primarily making use of the resources of its clearing members. These must pledge collateral for the transactions that they conduct (known as initial margins) and pay into a default fund as a supplementary insurance arrangement supported by all members to protect the system as a whole. The use of a CCP not only helps market participants to mitigate their

credit risk exposures to their counterparties, but also allows them to reduce their funding and capital costs by netting countervailing transactions in their overall portfolio.

CCPs usually have quasi-monopoly positions in sub-markets and, being systemically important financial market infrastructures, they cannot be readily replaced. Since the decision made by G20 leaders in Pittsburgh in 2009 to settle all standardised OTC derivatives transactions via CCPs, the importance of CCPs for the functioning of the financial system has increased further.⁴ This is why particular attention is being paid to CCPs at the national, European and international level, and also by the Bundesbank.

Revision of the regulatory framework

For CCPs, the international requirements were transposed into a legally binding regime at the EU level with the regulation on OTC derivatives, central counterparties and trade repositories

EMIR

³ This statement applies at least to losses which may arise in connection with the default of a clearing member.

⁴ See Deutsche Bundesbank, Increased importance of central counterparties, Financial Stability Review 2016, pp 79-90.

(European Market Infrastructure Regulation: EMIR⁵), which came into force on 16 August 2012 as well as with supplementary regulatory technical standards (RTS). With the EMIR, the CCPs in the EU were subject to a uniform supervisory and monitoring framework for the first time. The German CCPs – Eurex Clearing AG and European Commodity Clearing AG – received EMIR authorisation in April and June 2014, respectively. In addition to articulating supervisory requirements for CCPs, the EMIR also legally enshrines, amongst other things, the tasks and cooperation of the authorities in the supervision and authorisation of CCPs, the obligation to settle certain OTC derivatives via CCPs (clearing obligation) and also reporting obligations for derivatives contracts. The EMIR also provides recognition regimes for CCPs domiciled in non-EU countries wishing to offer services in the EU. One of the conditions for recognising such CCPs is that the non-EU country's supervisory and regulatory framework is equivalent to the EMIR.

*EMIR review
and REFIT*

Back in 2015, the European Commission began reviewing the regulatory framework, as envisaged in the EMIR. This review is also part of the European Commission's Regulatory Fitness and Performance Programme (REFIT) which aims to simplify European legislation and, in particular, to reduce bureaucracy and cut the costs to society as a whole.

Following the completion of this review, the European Commission put forward a proposal in May 2017 for a regulation to amend the EMIR.⁶ This proposal foresees just minor changes on balance. One is to simplify the existing rules on the suspension of the clearing obligation and to allow them to be applied more quickly than in the past, if necessary. Another is to create incentives for central clearing and improve access to CCPs. The proposal also aims to ensure greater transparency surrounding the calculation of collateral requirements by CCPs.

Proposals regarding the supervision of non-EU CCPs and the amendment of the CCP supervisory regime for EU CCPs

Furthermore, the importance of the CCP business has increased significantly, owing, *inter alia*, to the obligation to clear standardised OTC transactions via CCPs. On account of the global market structure, a concentration of CCPs in non-EU countries cannot be ruled out. The current recognition procedure no longer takes sufficient account of this. The problem of overseeing and supervising non-EU CCPs in Europe is being accentuated in particular by the forthcoming withdrawal of the United Kingdom from the EU ("Brexit"), as a large proportion of OTC interest rate and credit derivatives are currently cleared via CCPs in London. *EMIR II*

As things currently stand, UK CCPs still fall within the supervisory and regulatory perimeter laid down by the EMIR. Following the effective withdrawal of the United Kingdom from the European single market, a situation could arise where UK CCPs are automatically declared to be non-EU CCPs, unless subsequent arrangements are made in the meantime. Transactions conducted in the United Kingdom would then fall outside the common European supervisory and regulatory framework. This was one of the reasons why the European Commission put

⁵ Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories.

⁶ Proposal of 4 May 2017 for a regulation of the European Parliament and of the Council amending Regulation (EU) No 648/2012 concerning the clearing obligation, the suspension of the clearing obligation, the reporting obligations, the risk mitigation techniques for OTC derivatives contracts not cleared by a central counterparty, the registration and supervision of trade repositories and the requirements for trade repositories.

forward a further proposal in June 2017 for a revised version of the EMIR (EMIR II).⁷

Non-EU CCPs

The European Commission proposes making the future supervision of non-EU CCPs by EU authorities contingent on their classification in terms of systemic importance. In future, for example, the requirements for a non-EU CCP should vary according to its degree of systemic importance for financial stability in the EU as a whole or in one or more member states. For non-systemically important non-EU CCPs ("Tier 1" CCPs), the current procedure for assessing the equivalence of the supervisory and regulatory framework with the EMIR will continue to apply. However, systemically important non-EU CCPs ("Tier 2" CCPs) would have to meet key EMIR requirements and submit to extensive monitoring and information exchange rights of the European Securities and Market Authority (ESMA). A legal opinion should be available confirming that the ESMA is able to enforce these rights in the non-EU country. In the case of substantially systemically important CCPs, the European Commission could also, on the ESMA's recommendation, adopt an implementing act according to which such a CCP would only be allowed to offer its services within the EU if it is authorised to do so and is thus also domiciled in the EU ("location requirement"). This may be necessary in particular if the risks which a substantially systemically important non-EU CCP presents to financial stability in the EU or in an EU member state would not be sufficiently mitigated despite compliance with strict prudential provisions. From the Bundesbank's perspective, the three-stage approach of the European Commission generally provides an appropriate framework to take account of the varying systemic importance of CCPs.

Strengthening of ESMA should be viewed critically

The organisation of intra-European supervision is another area where the European Commission is proposing two major changes: strengthening the ESMA's role in the supervision of EU CCPs, and involving the relevant central bank of issue (CBI) to a greater degree. For ex-

ample, the national competent authorities for CCPs – in Germany the Federal Financial Supervisory Authority (BaFin) – would, in future, have to obtain the ESMA's approval for important decisions in connection with the supervision of CCPs. It is also proposed that a CCP Executive Session be set up within the ESMA, which would be responsible for general tasks related to CCPs and the supervision of EU CCPs and non-EU CCPs. From the Bundesbank's perspective, these proposals should be viewed critically as the approach adopted so far – besides only coming into force just a short time ago – has by and large proven its worth, and the innovations are likely to complicate, rather than simplify the supervisory regime.

The European Commission's proposal, on the other hand, which foresees giving the central bank of issue a greater role in future in terms of authorisation and ongoing supervision, is to be viewed differently. Since negative effects on the smooth functioning of payment systems, on the liquidity management of clearing participants and on the general liquidity situation on the money market need to be prevented, the greater say this proposal would give the CBI would have more of a bearing on the CCP's risk management. The Eurosystem already assumes the role of the CBI for the euro, mainly through participation in the existing EMIR colleges of supervisors for CCPs. For CCPs domiciled in the euro area, the Eurosystem is normally represented by the national central bank in the CCP's home country. For CCPs outside the euro area, this task is performed by the European Central Bank (ECB). In both cases, the CBI's decision-making process for the euro is carried out via the Eurosystem's decision-making bodies, the decisions of which are binding for the respective representative. Accordingly, the Bundes-

⁷ Proposal of 13 June 2017 for a regulation of the European Parliament and of the Council amending Regulation (EU) No 1095/2010 establishing a European Supervisory Authority (European Securities and Markets Authority) and amending Regulation (EU) No 648/2012 as regards the procedures and authorities involved for the authorisation of CCPs and requirements for the recognition of non-EU CCPs.

*Rights of the
Eurosystem and
the ECB*

bank represents the Eurosystem as the CBI in dealings with the German CCPs Eurex Clearing AG and European Commodity Clearing AG.

In order for the Eurosystem to be able to perform its role as a central bank of issue in accordance with the proposed revised version of the EMIR with legal certainty, the Governing Council of the ECB decided to issue a recommendation to the European Parliament and the Council of the European Union to amend the Statute of the European System of Central Banks (ESCB) and of the ECB⁸ in order to provide a clear legal basis for regulatory competences in the area of central clearing for financial instruments.

Recovery and resolution of CCPs

*Recovery and
resolution of
CCPs*

The increased importance of CCPs makes it all the more crucial to ensure that CCPs are secure and resilient in crisis situations. The minimum standards for CCP risk management laid down in the EMIR are generally designed to ensure that a CCP can cover the losses from the simultaneous default of the two clearing members with the largest risk positions under extreme but plausible market conditions. For this purpose, CCPs hold prefunded resources in the form of margins and a default fund. For more intense stress situations, there are currently only international standards and guidelines in place, according to which such losses must be covered but not prefunded. There are no statutory EU provisions, however. A forthcoming EU regulation for a recovery and resolution regime is to close this regulatory gap.⁹ Both the recovery and the resolution of a CCP are intended to safeguard financial stability and to ensure that the critical functions of the CCP are maintained, while minimising the use of public funds to protect taxpayers to as great an extent as possible. Regular insolvency proceedings, on the other hand, could jeopardise these objectives, since they would primarily serve to satisfy the insolvency creditors.

The viability of a CCP as a going concern can be jeopardised by two types of risk. The first involves losses from the default of clearing members which are unable to meet their financial obligations (default losses). The second relates to other losses such as those arising from operational or investment risks (non-default losses).

If a clearing member were to default, this would cause an imbalance in the CCP's otherwise matched book.¹⁰ This is generally why position allocation tools and loss allocation tools are needed. Position allocation tools may include the voluntary participation of clearing members in auctions or bilateral sales of the defaulting clearing member's positions. A further, enforceable position allocation tool is the close-out of positions of non-defaulting clearing members holding counter positions to the defaulting clearing member (tear-up or termination). Such close-out operations may result in losses that are not covered by the collateral¹¹ furnished by the defaulting clearing member or the additional amount of the CCP's dedicated own resources. Certain position and loss allocation tools are already provided for today as part of the regular default management framework, above all the use of resources from the prefunded default fund.¹² Other instruments are proposed in the European Commission's draft

*Risks to the
viability of a CCP
as a going
concern*

⁸ Recommendation for a Decision of the European Parliament and of the Council amending Article 22 of the Statute of the European System of Central Banks and of the European Central Bank (ECB/2017/18).

⁹ Proposal of 28 November 2016 for a regulation of the European Parliament and of the Council on a framework for the recovery and resolution of central counterparties and amending Regulations (EU) No 1095/2010, (EU) No 648/2012 and (EU) No 2015/2365. On 19 December 2017, a compromise proposal was published by the European Council: <http://data.consilium.europa.eu/doc/document/ST-15432-2017-INIT/en/pdf>. On 31 January 2018, a report was published by the European Parliament: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2018-0015+0+DOC+XML+V0//EN>

¹⁰ Losses not arising from the default of a clearing member can often only be covered by CCPs using their own funds.

¹¹ Initial margin and clearing member's default fund contribution.

¹² Known as the "default waterfall" in accordance with the EMIR.

Default waterfall and examples of measures for the recovery of a central counterparty (CCP)	
Default waterfall (prescribed by EMIR)	Position allocation tools: – Hedging of positions – Auctions and sale of positions on the open market Loss allocation tools: – Margins posted by the defaulting clearing member – Defaulting clearing member’s default fund contribution – CCP’s dedicated own resources – Non-defaulting clearing members’ default fund contributions
Additional measures from the recovery plan (agreed between the CCP and clearing members)	Position allocation tools: – Closure of positions (termination, full/partial tear-up) Loss allocation tools: – Cash call – Reduction in the CCP’s payment obligations (haircut)
Deutsche Bundesbank	

regulation, including the possibility of allocating losses by requesting cash calls from surviving clearing members (assignments) or applying haircuts to the variation margin gains of those clearing participants receiving payments from the CCP (gains based haircutting).

The table above provides an overview of the resources available to a CCP to cover losses associated with a member’s default pursuant to the EMIR as well as possible recovery measures should these resources prove insufficient.

The draft regulation stipulates that European CCPs will have to submit recovery plans in future which, in particular, include the identification of critical functions, the stress scenarios, a description of the recovery tools and the criteria for triggering their deployment.

While a default by a clearing member can normally be managed by a CCP autonomously, for the most part, as part of its risk management framework, implementing the more extensive measures needed for recovery, though likewise a matter for the CCP itself to handle, requires greater involvement on the part of the authorities. According to the draft regulation, recovery planning will involve the CCP’s competent supervisory authority and a college whose members are expected to include, *inter alia*,

the supervisory and resolution authorities for major clearing members. Not only would this take into account the interests and capabilities of the clearing members; it would also underline that responsibility for having adequate levels of risk provisioning lies with the clearing members and their respective competent authorities.

The resolution of a CCP, on the other hand, would be carried out by the competent resolution authority. The tools used for this purpose are, in some cases, identical to those used for a recovery. In addition to these, it is envisaged that the resolution authorities will have further tools at their disposal, such as the sale of business and bridge CCP tools.

Resolution of a CCP

Recovery plans and role of authorities

Central securities depositories

Central securities depositories (CSDs) provide important services for banks with regard to the safe custody, administration and settlement of securities which indirectly benefit banks’ customers. In the European Union, there are 28 national and two international CSDs. The oversight policy framework for CSDs prescribed by the international requirements is currently undergoing a major overhaul as a result of the

Central Securities Depositories Regulation

Central Securities Depositories Regulation (CSDR)¹³, which largely came into force in September 2014, and supplementary legislation at the European level. Much like the EMIR, the CSDR transposes the principles for financial market infrastructures into a single European supervisory and oversight regime for CSDs. In some respects, particularly in the area of settlement discipline, the CSDR even goes beyond the international requirements in terms of its content.

*Authorisation
under the CSDR*

In a reflection of the single European authorisation process which already exists for central counterparties under the EMIR, the CSDR now also establishes a similar arrangement for CSDs, according to which the CSD services defined in the CSDR are to be reviewed and evaluated in terms of risk. After the corresponding secondary legislation at the European level entered into force on 30 March 2017, CSDs had until 30 September 2017 to submit requests for authorisation. In Germany, Clearstream Banking AG Frankfurt (CBF) submitted its authorisation request in good time to BaFin – the competent national supervisory authority for securities. In formal terms, once BaFin has finished checking this request for completeness, it is to forward all the documents to the Bundesbank's oversight function, which then has up to three months to issue its opinion. In practice, BaFin and the Bundesbank liaise closely on this task, which includes preparing and checking the completeness of authorisation requests and reviewing their contents. Since CBF also has a banking licence, the Bundesbank is involved in this cooperative national supervisory and oversight regime in its function as a banking supervisor as well.

*Eurosystem's
CBI function*

As the euro ranks among the most important settlement currencies for the national CSDs located in the euro area, the Eurosystem, in its CBI function, is also to be involved in the authorisation processes for CBF alongside the Bundesbank. The Bundesbank will represent the Eurosystem as the CBI in dealings with CBF in much the same way as it does in matters of

CCP supervision. Within the Eurosystem, however, the Bundesbank will be bound by the rules of the Eurosystem's decision-making bodies in this respect. The Eurosystem's status as the CBI has ramifications beyond the authorisation process. Given that any monetary policy operations between banks and the Eurosystem have to be secured and the marketable assets either stored with or transferred to a CSD, the Eurosystem is an important user of the settlement services provided by CSDs. To date, the Eurosystem has carried out independent reviews and evaluations of the securities settlement systems operated by CSDs from a user's perspective. These will be discontinued in the foreseeable future as their content overlaps with the provisions of the CSDR to a large extent. It is envisaged that the insights into the risk situation gained through the Eurosystem's CBI role will be used in future to assure the suitability of the CSDs concerned for the Eurosystem's monetary policy operations.¹⁴

From a legal perspective, the TARGET2-Securities (T2S) platform¹⁵ operated by the Eurosystem is neither a CSD nor a securities settlement system, which means that it does not fall within the immediate scope of the CSDR. As a technical platform for securities settlement in central bank money, T2S does provide central services for participating CSDs, however. The indirect impact of this is that T2S must enable participating CSDs to comply in full with the CSDR requirements.

CSDR and T2S

Established by the European Commission in 2016, the European Post-Trade Forum (EPTF) is expected to play an important role in removing

EPTF

¹³ Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012.

¹⁴ In this context, it was also necessary to make modifications to the Guideline on the implementation of the Eurosystem monetary policy framework, with the amendments applying from 18 April 2018. See Article 2 of Guideline ECB/2018/3 of 7 February 2018.

¹⁵ For more information, see Deutsche Bundesbank, The Eurosystem's financial market infrastructure – origin and future set-up, Monthly Report, December 2017, pp 69-88.

any remaining post-trade barriers to the integration of European financial markets and the full implementation of a European capital markets union.¹⁶ The expert group's report of 15 May 2017 discusses the "Giovannini barriers"¹⁷ in greater detail and provides an overview of lingering and newly identified barriers. Building on this report, the EPTF carried out a public consultation from 23 August until 15 November 2017 to identify trends in post-trade services, dismantle market barriers and better manage existing risks. The ultimate objective of all of these efforts is to make the European post-trade landscape even more efficient, more competition-oriented and, above all, safer. Another topic on the EPTF's agenda is how new technologies (eg blockchain) and the services provided by innovative FinTech companies impact on securities settlement.

Systemically important payment systems

SIPS Regulation

In July 2014, the ECB exercised its authority to issue regulations in the area of payment systems oversight¹⁸ for the first time. The Regulation on the oversight requirements for systemically important payment systems (SIPS Regulation)¹⁹ governs responsibilities, rights and obligations in the oversight of systemically important payment systems. Like the CSDR, the SIPS Regulation goes beyond the international standards in terms of its requirements. For instance, systemically important payment systems are expected to ensure that final settlement takes place in central bank money at the end of the day.

Systemic importance and tasks of oversight authorities

Systemic importance is measured here using a combination of different criteria: the value of the payments settled, market penetration, the scope of cross-border activity, and use by other financial market infrastructures (see the chart on page 50). Once a year, the Eurosystem conducts a review to determine which payment systems are considered systemically important within the meaning of the SIPS Regulation and

nominates a competent oversight authority in the Eurosystem for each system meeting the criteria. This authority is responsible for monitoring the compliance of the payment system with the SIPS Regulation and has the right to obtain information from the system operator as well as to issue recommendations for corrective action if necessary. Should breaches of the Regulation be identified, the ECB has the power to impose sanctions on the system operator.

In August 2014, the Eurosystem classified four payment systems as systemically important (see the table on page 50): TARGET2, the payment system operated by the Eurosystem, and the commercial systems EURO1, STEP2-T and CORE(FR). The Banque de France was nominated as the competent authority for CORE(FR), while the ECB is responsible for the other systems. The Bundesbank assists the ECB with these oversight activities in the Eurosystem. The retail payment system operated by the Bundesbank, on the other hand, does not meet the above-mentioned criteria. It falls into the category of other retail payment systems which only have to observe selected rules in certain areas.

November 2017 saw the ECB Governing Council approve amendments to the SIPS Regula-

Revision of the SIPS Regulation

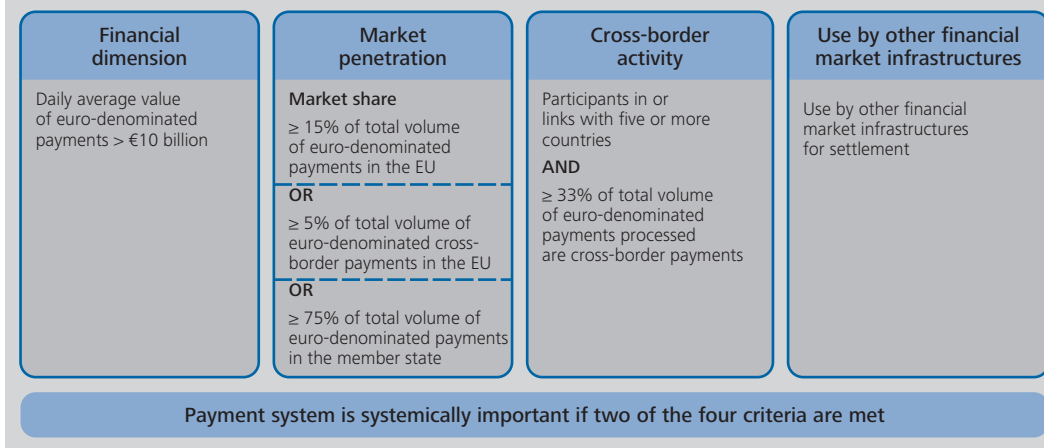
¹⁶ The ESCB only has observer status in the EPFT. The EPFT's members are primarily representatives from various interest groups and independent experts.

¹⁷ The origins of this term can be traced back to the Giovannini Group, a group named after its chairman Alberto Giovannini, which published reports between 2001 and 2003 on cross-border clearing and settlement arrangements in the EU securities markets and identified various barriers (https://ec.europa.eu/info/publications/giovannini-reports_en).

¹⁸ The oversight of payments and settlement systems is a central bank task aimed at promoting security and efficiency. The central bank monitors existing and planned systems, reviews their security and efficiency, and ensures that changes are made where appropriate. For more information, see Deutsche Bundesbank, Payment system oversight – a contribution to the stability of the financial system and the efficiency of payment operations, Monthly Report, January 2004, pp 29-44.

¹⁹ Regulation of the European Central Bank (EU) No 795/2014 of 3 July 2014 on oversight requirements for systemically important payment systems (ECB/2014/28).

Criteria for determining a payment system's systemic importance



Deutsche Bundesbank

tion²⁰ which mainly comprise more stringent rules for credit and liquidity risk assessment, new cyber resilience requirements and new powers for competent oversight authorities. In future, overseers will be able to appoint an expert to perform an independent review of the system, which means that individual elements can be assessed in detail if, for example, the competent authority itself does not have the necessary expertise. The competent authority can also conduct on-site inspections.

Cyber resilience

The revision also reflects the Eurosystem's focus on the increased threat posed by cyber risks in

recent years, although it does not spell out how cyber resilience is to be achieved in detail. Having said that, the Committee on Payments and Market Infrastructures (CPMI) and the International Organization of Securities Commissions (IOSCO) already published their *Guidance on cyber resilience for financial market infrastructures*²¹ back in June 2016. This document outlines general objectives for strengthening cyber resilience, and leaves scope for the relevant financial market infrastructure to determine how these objectives may be achieved individually. The key aspects of the guidance document are as follows.

Payment volumes in systemically important payment systems*

2016, total

SIPS	Number of transactions (in millions)	Value of transactions (€ billion)
TARGET2	89.0	485,811.8
EURO1	53.3	41,103.6
STEP2-T	10,419.0	13,169.3
CORE(FR)	14,432.2	5,513.0
Total	24,993.5	545,597.7

* Source: Statistical Data Warehouse of the ECB.

Deutsche Bundesbank

- Cyber resilience should also receive due attention from the FMI's board and senior management.
- The ability to resume operations quickly and safely following a successful cyber attack should be top priority.
- Cyber resilience should be tested regularly and information on the threat environment analysed.

²⁰ Regulation (EU) 2017/2094 of the European Central Bank of 3 November 2017 amending Regulation (EU) No 795/2014 on oversight requirements for systemically important payment systems (ECB/2017/32).

²¹ See also <https://www.bis.org/cpmi/pub/d146.htm>

- The importance of cyber resilience should be reflected in the company culture.
- Improvements in cyber resilience require the joint efforts of the industry as a whole.

The Eurosystem has since formulated specific oversight requirements for the guidance document's application in the euro area. These requirements are currently open for public consultation.²² They exist not only to assist oversight authorities in reviewing financial market infrastructures, but also to outline detailed steps for infrastructure operators to improve cyber resilience and to encourage the achievement of this objective through dialogue and close cooperation between operators and oversight authorities.

■ Payment services

PSD2 ...

In 2009, the Payment Services Directive (PSD) formed a harmonised legal framework for the settlement of payments in the EU. The revised version of this legislation (PSD2²³) is now expected to be a catalyst for major change in the payment services market.

In its revised form, the PSD2's objectives are, on the one hand, to further deepen market integration within the European Union and help strengthen competition and consumer rights. On the other hand, new rules are expected to add to the security of retail payments, especially with regard to the use of innovative payment methods such as payments made using a mobile phone.

... transposed into national law since January 2018

The PSD2 had to be transposed into national law by 13 January 2018. This was done in Germany, *inter alia*, through amendments to the Civil Code (*Bürgerliches Gesetzbuch*) and the Payment Services Oversight Act (*Zahlungsdiensteaufsichtsgesetz*) via the Act implementing the provisions of the Second Payment Services Directive of 17 July 2017, which entered into force on 13 January 2018.

One key amendment of the PSD2 is the addition of payment initiation services (PIS) and account information services (AIS) to the list of payment services. While providers of PIS initiate customers' credit transfer orders from payment accounts held with their payment service provider (particularly where e-commerce purchases are paid for), providers of AIS make available to their customers consolidated information on one or more of their payment accounts held with other payment service providers (PSPs). With the introduction of the PSD2, the interaction between account servicing payment service providers (ASPSPs) and these third-party providers, which have been in the market since the mid-2000s, is now governed by law.

New payment service providers ...

The inclusion of an additional service provider in the PIS and AIS process chains between the customer and the ASPSP meant that the existing rules needed to be amended and new ones introduced. The resulting changes relate to both the specific rights and obligations which the new entrants have towards their customers, such as the handling of confidential customer data, and also to the rules concerning their relationship with the ASPSPs, particularly with regard to identification requirements and secure communications. The existing transparency and disclosure requirements for PSPs, however, have been left largely unchanged.

... prompt new rules

Lastly, in addition to strengthening consumer rights, the PSD2 also contains a raft of new rules to increase the security in retail payments and improve the protection of customers' financial data. Perhaps the most important of these is the requirement for PSPs to use strong

More security in retail payments

²² See ECB press release of 10 April 2018, ECB launches public consultation on cyber resilience oversight expectations.

²³ See also Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

Strong customer authentication

Requirements of strong customer authentication

- Generation of an authentication code based on at least two independent elements from different categories (knowledge, possession, inherence)
- For remote payments, dynamic linking of the authentication code to payment amount and payee

Exemptions from strong customer authentication

- Access to account information without disclosure of sensitive payment data
- Contactless payment transactions at the point of sale of up to €50
- Transport fares and parking fees at unattended payment terminals
- Remote electronic payments to trusted beneficiaries/as recurring transactions (same payee and payment amount)/to the same natural or legal person/of up to €30
- Corporate payments based on secure payment processes and protocols
- Payment transactions posing a low level of risk according to real-time transaction risk analysis

Measures for the protection of personalised security credentials

- Ensure the confidentiality and integrity of authentication codes during all phases of the authentication
- Ensure the confidentiality and integrity of personalised security credentials throughout their lifecycle

customer authentication.²⁴ Strong customer authentication has to be applied when a customer (a) accesses their payment account online, in other words via the internet or a mobile device, (b) initiates an electronic payment, or (c) carries out any action through a remote channel which may imply a risk of payment fraud or other abuse. For remote electronic payments, strong customer authentication must also include elements that dynamically link the payment transaction to the respective payment amount and payee.

In key areas, the PSD2 contains only general provisions, which still need to be fleshed out. To this end, the PSD2 assigned the European Banking Authority (EBA), in cooperation with the ECB, three mandates to draw up regulatory technical standards (RTS) and guidelines.²⁵

The debate surrounding the EBA's RTS for strong customer authentication and secure communication has attracted particular attention. The EBA drew up these RTS in cooperation with the ECB and several central banks from the European Economic Area, including the Deutsche Bundesbank. They were published by the European Commission as a delegated act on 13 March 2018 and provide further details – ensuring technology and business-model neutrality – concerning the type of authentication that PSPs have to require from their customers as well as possible exemptions to the application of strong customer authentication (see the adjacent box). Furthermore, they also include provisions on the protection of personalised security credentials and on the design of common and secure standards for communication between the dif-

Mandates for the European Banking Authority

Regulatory technical standards for strong customer authentication and secure communication

²⁴ In accordance with Article 4 (30) PSD2 and section 1 (24) of the Payment Services Oversight Act, strong customer authentication requires at least two independent factors from two out of three categories: "knowledge" (= something only the user knows, such as a password), "possession" (= something only the user possesses, such as a payment card) and inherence (= something that the user is, such as a fingerprint).

²⁵ A further eight mandates are of a purely banking supervisory nature and assigned exclusively to the EBA.

ferent PSPs as well as between PSPs and their customers.

The core of this second part of the standards is the obligation for ASPSPs to provide at least one interface to the customer account for payment initiation service providers (PISPs) and account information service providers (AISPs). This access to payment accounts can take place through the customer's existing online banking interface or via a new dedicated interface, known as an application programming interface (API), and requires the third-party PSP to identify itself to the ASPSP. If the ASPSP opts to have a dedicated interface, this interface must offer the same level of availability and performance as access via the customer interface. Furthermore, ASPSPs opting for an API have to provide a contingency fallback mechanism via which PISPs and AISPs can access the customer account, also after having identified themselves to the ASPSP. However, an ASPSP may, under certain conditions, be relieved of this obligation by its national supervisory authority. The RTS will enter into force 18 months after publication. For those payment accounts covered by the PSD2, this will also put an end to the current practice of PISPs and AISPs accessing customer accounts without prior identification.

In December 2017, the EBA adopted guidelines on security measures and control mechanisms to contain the operational and security risks of payment services. Taking into account the principle of proportionality, the EBA and the ECB developed requirements, including some pertaining to governance, risk assessment, protection of data and systems, business continuity and testing, in line with the existing EBA guidelines on the security of internet payments and with other standards and frameworks. The new rules have a wider scope than the existing EBA guidelines as they apply to all providers and payment services that are covered by the PSD2. They shall be implemented by the national supervisory authorities in their respective supervisory practices.

The guidelines on major incident reporting entered into force on 13 January 2018. They require PSPs to report relevant incidents to their competent supervisory authority. In Germany, this is BaFin, which forwards the reports to the Bundesbank, the EBA and the ECB, and – if the incident is of relevance – also notifies other national authorities.

In addition to the PSD2 and its downstream acts, other European rules and projects have a significant influence on the provision of payment services. They include, for example, the Fourth Money Laundering Directive and the new Regulation on information accompanying transfers of funds, which, in line with current international standards and recommendations, modernise the legal framework to combat money laundering and terrorist financing.²⁶

This results, *inter alia*, in changes in customer identification, such as when consumers open a payment account electronically. For instance, under the German legislation transposing the Fourth EU Money Laundering Directive on authentication of online services, electronic identification means as defined in the Regulation on electronic identification and trust services for electronic transactions²⁷ are also accepted under certain conditions. This can be, for example, an electronic identity card or a chip card containing data that is used to identify a person. The German transposition also mentions the possibility of using video identifi-

Guidelines on major incident reporting

Prevention of money laundering and terrorist financing ...

... promotes support for digital business processes through electronic identification

Guidelines on the management of operational and security risks

²⁶ See also Directive (EU) 2015/489 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC as well as Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006.

²⁷ Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. According to Article 3 (2) of the Regulation, an electronic identification means is "a material and/or immaterial unit containing person identification data and which is used for authentication for an online service".

“Consumer Financial Services Action Plan: Better Products, More Choice”

cation procedures. BaFin has already outlined requirements for the use of such procedures for institutions operating in Germany. These developments can help fully digital business processes become more firmly established and thus capitalise to an even greater extent on the potential offered by digitalisation.

Lastly, in March 2017, the European Commission published the “Consumer Financial Services Action Plan: Better Products, More Choice”. Concrete action followed on 28 March 2018 in the shape of a Commission proposal stating that, in the future, charges on cross-border payments in euro should be set at the level of domestic payments for the EU as a whole. To date, this regulation has only applied to euro area countries. The proposal also aims at increasing transparency for payments involving a currency conversion, thus boosting competition.²⁸

■ Conclusion

Resilient financial market infrastructures are of paramount importance for both the financial system and the real economy, given their central role in settling financial transactions. Disruptions to these critical components can have significant implications for the participating banks, for financial markets and for the performance of tasks by the Eurosystem. One reason for this is that central banks rely heavily on the services of CSDs to receive collateral for monetary policy loans to counterparties or to hold securities under the current purchase programmes. In addition to effective supervision and oversight, the provision of settlement services in highly liquid and highly secure central bank money is also crucial to reducing risks and safeguarding financial stability.

In view of the heightened threat situation, strengthening the cyber resilience of financial market infrastructures has a particularly high priority for supervisory and overseeing authorities. In this context, it is essential to give due

consideration to the fact that while advancing digitalisation means efficiency gains, it also opens up new points for attack and changes the risk situation for market infrastructure operators. Responsibility for taking action to raise the level of protection lies primarily with the system operators and market participants themselves. But it is not simply a matter of implementing suitable technical devices – risk awareness has to become part of the corporate culture. Given the rapid pace of change, supervisors are applying a new approach; rather than monitoring whether specific provisions have been fulfilled, they instead analyse the degree of maturity of the defensive measures in place and steps being taken to improve them. In addition, the Eurosystem has made a valuable contribution by setting up the European Cyber Resilience Board (ECRB). The aim of this board is to promote dialogue on cyber resilience among European financial market infrastructures, central banks and other regulators.

Other key points to be addressed concern CCPs. Central clearing has experienced a veritable boom in recent years. As a result, efforts should be stepped up to complete the work on the European recovery and resolution regime for CCPs in the near future. The aim must be to establish a credible regime that ensures financial stability and, in the event of a serious occurrence, manages as far as possible without having to resort to using public funds. For the Bundesbank, it is essential that the future supervisory regime for non-EU CCPs is based on functioning supervision by the authorities of the EU member states in compliance with regulations valid across the EU. Accordingly, when assessing concrete policy options, precedence must be given to ensuring that payment transactions and the settlement of securities and derivatives transactions are secure, with cost considerations taking second place. In any event,

²⁸ Proposal for a regulation of the European Parliament and of the Council amending Regulation (EC) No 924/2009 as regards certain charges on cross-border payments in the Union and currency conversion charges SWD (2018)84.

due to the multiple interactions with its tasks, the Eurosystem should be appropriately involved in supervision.

The PSD2 substantially amends the rules governing EU payment transactions. Well-established structures in the market for payment services are likely to be broken down as a result, in particular, of the possibility for third parties to offer customers innovative services on the basis of access to their accounts (known as “open banking”). The Bundesbank is of the opinion that the rules outlined in the PSD2 as well as the related RTS provide a good basis for the further digitalisation of payment transactions, in particular by increasing competition and ensuring that security levels are high. Consistent implementation of the PSD2 and application of the RTS across all member states are

essential in order to stimulate competition throughout the EU and overcome fragmentation in national markets. In addition, care must be taken to ensure that the provision of dedicated interfaces (APIs), which both third-party PSPs and other credit institutions can access, in the banking industry is sufficiently standardised. Only then will it be possible for new and attractive products for consumers to grow and thrive in the Single Euro Payments Area. At this stage, it is difficult to say whether these new products will be brought to the market more by traditional credit institutions, start-ups or existing internet platforms. However, the leading credit institutions appear to have recognised that the PSD2 does indeed offer scope to increase the service level of the payment account they offer their own customers, and to thus enhance their own attractiveness.