NATIONAL BANK OF SERBIA

PAYMENT SYSTEM DEPARTMENT

PAYMENT SYSTEM OVERSIGHT

2015 and the first half of 2016

Contents:

Introduction

The National Bank of Serbia maintains payment systems and promotes the objectives of soundness, safety and efficiency by assuming the role of operator, development catalyst and, in particular, the overseer/supervisor of payment systems. These roles of the NBS are intertwined and complementary, reaching towards the same goal – safe and efficient payment systems in the Republic of Serbia.

In conducting payment systems supervision/oversight, the NBS is guided by the following principles:

- transparency,
- application of internationally accepted standards for payment systems,
- consistent application of requirements and standards to comparable payment systems.

By reporting annually on its oversight activities, the NBS ensures transparency and contributes to a better understanding of the requirements and standards that payment systems need to comply with.

The application of the new Law on Payment Services[1] began in 2015, and in the first half of 2016 the NBS adopted a set of supporting regulations necessary for the implementation of provisions which regulate payment systems.

Activities of the NBS in the performance of payment system supervision/oversight in 2016 focused on the verification of compliance with requirements for the issuance of licences for payment system operation to legal entities that managed payment systems in accordance with the Law on Payment Transactions and regulations under that Law, and to new participants in the Serbian market.

[1] RS Official Gazette, No 139/2014.

1 Objectives and scope of payment system supervision/oversight

Primary objectives of supervision/oversight of payment systems are stability and security of operations and adequate management of risks in these systems.

Safe and sound functioning of an individual payment system is the responsibility of that system's operator that should create an environment conducive to making appropriate business decisions by understanding the identified risks and the consequences they can cause to the operation of a payment system.

However, the NBS needs to make sure that payment systems are reliable regardless of the operator, hence supervision/oversight includes off-site and on-site supervision of payment systems operation and the monitoring of their compliance with the Law on Payment Services and regulations adopted under that Law.

It is primarily payment systems themselves that are the scope of supervision/oversight, while the activities within this function are focused on the operation of the systems as a whole, rather than of the individual participants.

The scope of oversight also includes payment instruments which are used to initiate payment transactions in payment systems – if the use of those instruments is governed by particular rules agreed between their issuers. Overseeing the use of payment instruments is an important part of the oversight of payment systems in which payment transactions are initiated by those instruments and includes chiefly the consideration of the safety of their use, which is important for the maintenance of the public's confidence in the national currency.

2 Regulatory framework

A payment system is an infrastructure of the financial market used for the transfer of funds between market participants, which has written and standardised procedures and rules for processing and netting and/or settlement of transfer orders applying to all system participants. Safe and sound payment system operation is important not only for system participants, but also for end-users of payment services.

The NBS performs the supervision/oversight of payment systems in accordance with the Law on the National Bank of Serbia,[2] the Law on Payment Services and the regulations adopted under that Law.

The Law on the National Bank of Serbia (Articlec 4 and 59) sets out that the NBS:

- regulates, supervises and promotes smooth performance of domestic and cross-border payment transactions, in accordance with law;

[2] RS Official Gazette, Nos 72/2003, 55/2004, 85/2005 – other law, 44/2010, 76/2012, 106/2012, 14/2015 and 40/2015 – CC decision.

- issues and revokes operating licenses to and from payment system operators, supervises their operations and performs other activities, in accordance with the law governing payment services;
- ensures safe and efficient functioning and development of payment systems and, in accordance with law, enacts regulations governing those systems.

Pursuant to the authorisation referred to in the Law on Payment Services, the NBS adopted the following supporting regulations:

- Decision on the Conditions and Manner of Granting License for Payment System Operation and Granting Approval for Amendments and Supplements to Payment System Rules (RS Official Gazette, No 49/2015);
- Decision on the Manner of Maintaining and Enhancing Safe and Sound Payment System Operation and Reporting to the National Bank of Serbia (RS Official Gazette, No 49/2015);
- Decision on the Content and Manner of Maintaining Records of Payment Systems (RS Official Gazette, No 49/2015);
- Decision on Initial Capital and Minimum Amount of own Funds of a Payment System Operator (RS Official Gazette, No 49/2015);
- Decision on Detailed Conditions and Manner of Supervision of Operations of Payment Systems (RS Official Gazette, No 49/2015).

The Law and the above supporting regulations enhanced the regulatory framework for payment systems, particularly with respect to laying down requirements for ensuring safe and sound functioning of those systems, efficient management of risks to which these systems are or could be exposed, and implementation of supervisory requirements for systemically important payment systems[3] with the necessary adjustments to comply with the domestic market.

2.1. Key aspects of the regulatory framework

The Law regulates payment systems in a thorough, complete and clear manner. Seeking to ensure safe and sound operation of a payment system, the Law imposes requirements on the system operator relating to organisational, staffing and technical aspects, the system of governance and internal controls, and the continuous management of risks in the payment system, in particular the financial and operational risk.

[3] Regulation of the ECB (EU) No 795/2014 of 3 July 2014 on oversight requirements for systemically important payment systems (ECB/2014/28).

The key aspects of the regulatory framework for payment systems relate to the understanding of:

- operations performed in a payment system and the terms related to them as specified by the Law;
- the idiosyncrasies of risks that may occur in a payment system;
- the importance of payment system operating rules which the operator of the system follows in its operation.

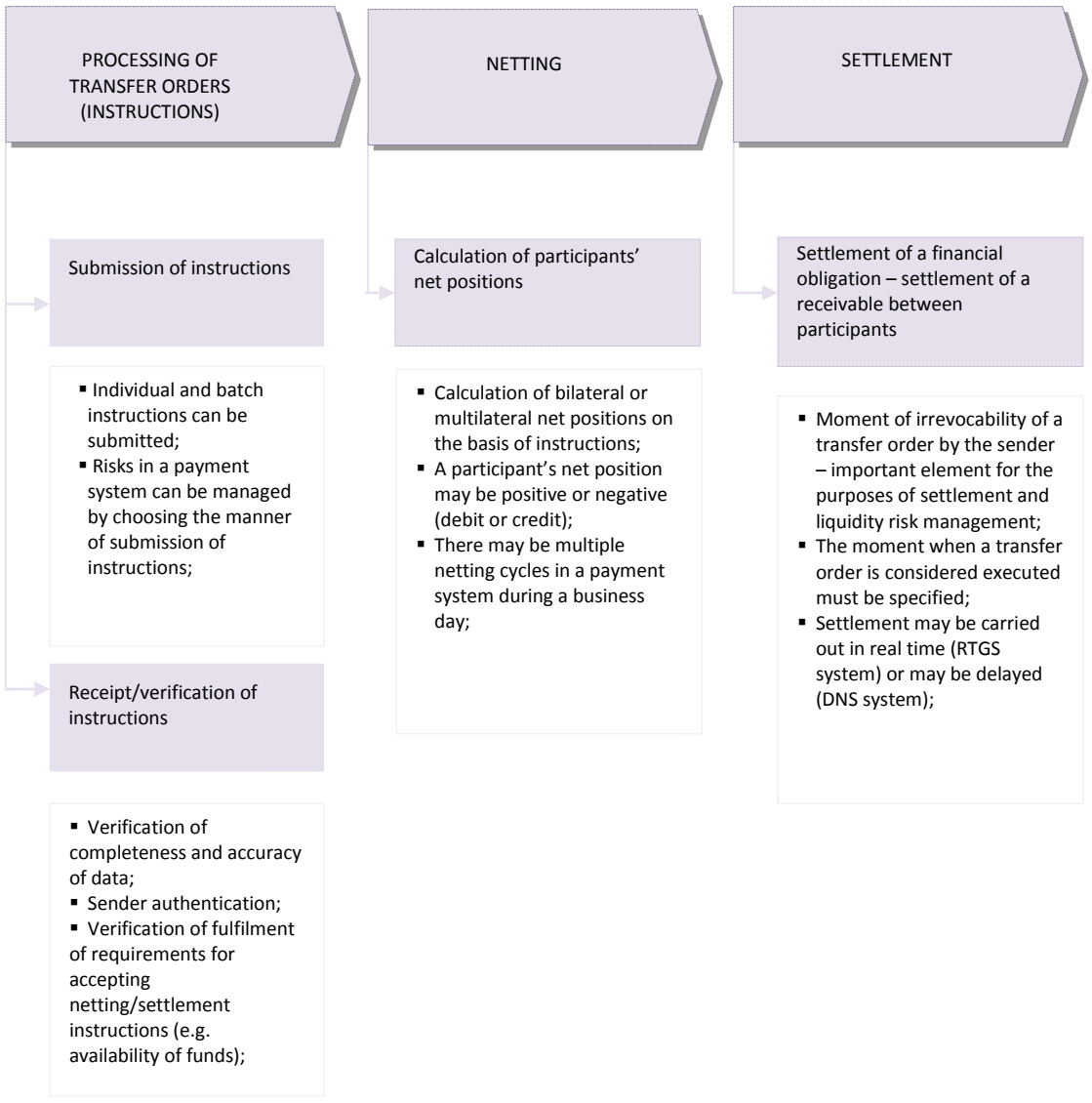
2.1.1. Payment system activities

Funds are transferred between payment system participants in accordance with standardised procedures and rules for processing and netting and/or settlement of transfer orders which apply to all participants in that system. In view of this, primary activities in a payment system are processing of transfer orders, netting and/or settlement based on those orders.

A transfer order in a payment system is an instruction by a participant in that system to place an amount of funds at the recipient's disposal or an instruction resulting in a discharge of payment obligations between participants in the payment system. This instruction primarily arises from a payment service that participants – payment service providers provide to their beneficiaries.

For participants to understand the risks they assume by participating in a payment system, the "life cycle" of a transfer order, i.e. the execution of that order must be presented in a completely transparent, accurate and comprehensive manner. Chart 1 shows the stages a transfer order goes through during execution in a payment system.

Chart 1 Stages in the execution of a transfer order in a payment system



The first stage in the execution of transfer orders in a payment system is the submission of those orders (instructions). Participants may be offered various ways to submit these orders (e.g. individually or in a batch). This process is usually automated in payment systems. Numerous factors determine the submission of transfer orders by participants, e.g.: requirements set out in regulations, the daily time schedule of the payment system, liquidity costs, risk management, payment system technology in terms of whether there is a queue, the ability to specify and change the priority of instructions, etc. Net positions from other payment systems may be settled using various models for submission of transfer orders (e.g. all orders for crediting and

debiting participant accounts in respect of net positions are submitted simultaneously, etc.).

After submission, the transfer order is subject to various verifications prior to receipt/acceptance for netting/settlement. The type of verification carried out in the payment system depends on the type of system and the technology it operates on, but primarily includes the verification of completeness and accuracy of certain data in the transfer order, and of authenticity of its sender with the aim of ensuring integrity and irrevocability of the transaction (transfer order validation). If the system is unable to verify that a transfer order is valid, the order is usually rejected and returned to the participant – sender and is not accepted. If the verification is successful, the transfer order enters the second stage where a new verification is conducted to determine whether the transfer order meets certain requirements for acceptance for netting/settlement. Most commonly, this relates to the verification of availability of funds for settlement and, in some cases, for netting, depending on whether the system is a RTGS[4] or DNS[5] system. If the transfer order does not meet this requirement, the system may reject that order or temporarily move it to the queue (if the payment system has this function), which it will leave once the requirement is met.

In a DNS system, a transfer order is first included in netting (calculation of net positions of participants – bilateral and multilateral net positions), after which the calculated net positions are settled.

Settlement means the settlement of a financial obligation or the settlement of a receivable between payment system participants based on a transfer order and is performed by transferring funds. The moment when a transfer order in a payment system is considered executed depends on the legal framework in which the payment system operates, and in particular on the operating rules of the payment system.

In some payment systems the sender may not recall a transfer order if the order has undergone validation, which means that the sender may not recall the order even though e.g. the order was queued (in payment systems supporting this function), whereas in other payment systems the sender may recall a transfer order at any time before settlement (RTGS) or the moment when the calculation of net positions begins (DNS).

An integral feature of the RTGS system technology is the performance of settlement without delay, after the verification of a transfer order and if the requirement relating to the availability of a participant's funds has been met.

In a DNS system, transfer orders are generally considered executed once net positions calculated in respect of those orders are settled. In this type of system there are numerous mechanisms for managing financial risk, which are selected based on the assessment of exposure of the payment system to this risk and on whether the payment system is defined as important for the financial market (these mechanisms include e.g.

[4] RTGS – Real Time Gross Settlement System.
[5] DNS – Designated-time Net Settlement Systems.

introduction of multiple net position netting and settlement cycles, prefunding for maximum negative net position, net position unwinding and similar).

2.1.2. Risks in a payment system

Risks that may occur in a payment system are specific and relate to negative effects on payment system operation. In this context, financial and operational risks are the most important.

Financial risks in payment systems arise from uncertainty regarding the ability of a participant or another entity to manage their liquidity (liquidity risk) and to meet their settlement obligations (solvency risk).

Operational risks in payment systems arise from omissions of employees, deficiencies in information and other systems, inadequate internal procedures and processes, as well as the occurrence of unforeseeable external events.

In addition to risk management being important for safe and sound operation of a payment system, it is also important for the achievement of the defined objectives of operators. Risk management is particularly significant in important payment systems where risk materialisation can "spill over" and jeopardise the stability and confidence in the financial system (systemic risk). On the one hand, centralisation of some activities in a payment system enables its participants to more efficiently and effectively manage their risks, but on the other hand, it breeds interdependence between various entities relevant to the operation of this system and therefore to risk concentration.

A payment system is primarily exposed to financial risk arising from its participants. The system's operating rules and the procedures applied are crucial for managing this risk. Some payment systems are not exposed to solvency risk – due to the technology they are based on, RTGS systems do not face solvency risk arising from their participants; however, they are exposed to high liquidity risk, given that participants need to have sufficient liquidity at their disposal to smoothly execute transfer orders. Conversely, transfer orders in a DNS system may be processed in real time, but the calculated net positions are settled with a delay, which exposes the participants to financial risk during the delay period.

Negative effects on the operation of a payment system may also stem from the settlement agent due to e.g. his/her inability to meet all of his/her obligations, or an inability to settle due obligations – if settled funds are not immediately available to participants upon settlement of payment. In this regard, the payment system operator should adequately manage financial risk to which the payment system and its participants are exposed due to the selection of the settlement agent. This risk is eliminated by selecting the NBS as the settlement agent, whereas the Law prescribes

that only the NBS can be the settlement agent of important payment systems, given their systemic importance.

On the other hand, a payment system can also be negatively impacted by the materialisation of solvency or liquidity risk on the part of the system operator. An operator may jeopardise the operation of a payment system by inadequately managing the overall operational risk. Liquidity risk management is particularly important to ensure coverage of operating costs in relation to the payment system in the period planned for the recovery or cessation of operations of a payment system and the establishment of or transfer of participants to an alternative manner of execution of transfer orders.

All payment systems are exposed to operational risk, which may lead to a delay in the execution of transfer orders, financial loss, liquidity problems and damage to the system's reputation. Consequences of operational problems are particularly dangerous in important payment systems and may threaten the stability of the financial system as a whole.

Key factors in operational risk management include: information system safety, operational reliability and business continuity in a payment system. Use of good business practices and commonly accepted standards in the field of information system safety and business continuity enables the operator to set up an appropriate framework for operational risk management. Internal and external sources of this risk include e.g. inappropriate identification and understanding of risks and control activities and procedures necessary to manage this risk, inappropriate control of the system and processes, cessation of provision of services of other persons (telecommunication services, electricity supply), natural disasters etc. As the payment system is a complex infrastructure, its operational reliability depends on the operational reliability of all components involved in its operation. Defining the degree of operational reliability may differ depending on the manner of settlement (RTGS or DNS system). In general, operators should pay particular attention to the telecommunication infrastructure, as its operational reliability is essential for payment systems. Where possible, the level of services, alternative communications channels and other factors should be specified in a contract with the telecommunication services provider.

The operator also needs to set up procedures including the identification, analysis, resolution and documenting of incidents in a payment system. To maintain the defined level of operational reliability, the operator must ensure that any changes to the information system of the payment system are tested and approved prior to putting into operation and that appropriate procedures and a plan for returning the system to a previous state are introduced in relation to this.

To ensure that participants are able to appropriately manage risks to which they are exposed by participating in a payment system, the operator should provide them on time with accurate and complete data and information required for the risk management process, which include all necessary technical documentation, manuals,

etc. It is also important that the operator cooperates with the participants in making decisions regarding payment system operation and management of risks in the system, and in particular those decisions that relate to its operating rules, so as to ensure that the needs of the payment system are met efficiently and effectively.

Given the significance of important payment systems, in addition to the requirements prescribed for all payment systems, these systems must meet additional requirements prescribed by the Law and supporting regulations, e.g. operating rules of an important payment system must clearly define the moment of acceptance of a transfer order in that system and the moment after which the participant and the third party may not revoke the order (moment of irrevocability). The operator needs to undertake all reasonable measures to ensure the continuation of core operating processes relating to the operation of the payment system within two hours of the occurrence of events preventing regular operation of the system, and to ensure the completion of settlements based on transfer orders by the end of the day when the settlement must be performed at the latest.

2.1.3. Operating rules of a payment system

Payment systems have specific characteristics and are important for a country's economy, thus their functioning needs to be regulated so as to reduce the possibility of systemic shocks and ensure the stability of the overall financial infrastructure. A transparent and reliable legal framework and the availability of necessary information are preconditions for establishing and comprehensively managing a payment system, for the purposes of identification, assessment and monitoring, as well as of making decisions on measures for handling all types of risks that may occur in payment systems.

Since a payment system is established by concluding a written agreement/contract among the system's participants or between the participants and the operator of the payment system, and since its operations are based on standardised procedures and simple rules for executing transfer orders and the operator is responsible for the system's operation, clear rules, processes and procedures for the system's operation need to be defined. In view of this, to better understand and efficiently apply the Law and supporting regulations regarding payment systems, it is important to lay down some guidelines, particularly with respect to the system's operating rules. These guidelines are recommendations – minimum expectations that operators need to meet when establishing a payment system. The guidelines are also a source of information to potential participants and all interested parties about the payment system design (characteristics) and the risks they would incur by participating in the system. Also, in this way the NBS complies with the principle of transparency in the performance of payment system supervision by providing a basis for the assessment of the

performance of this function, in line with the recommendations of relevant international institutions.[6]

Operating rules of a payment system govern its operation by presenting its basic design in a comprehensive, clear and accurate manner and by regulating standardised procedures for processing and netting and/or settlement of transfer orders in that payment system. A payment system's rules are meant to be adhered to both by the system's participants and its operator in the execution of payment transactions.

The operator of a payment system is a legal person that submits a request to the NBS for approval to operate a payment system and that, upon receiving the approval, becomes responsible, in accordance with the Law, for managing the payment system's operation. The operator should provide legal certainty in all segments of the payment system's operations, while observing the regulations governing payment systems.

The operator is obliged to ensure safe and sound functioning of the payment system which at the time of its establishment greatly depends on how clear and applicable its operating rules are, without prejudice to the operator's responsibility for managing risks that may occur in the payment system after the beginning of its operation.

Above all, operating rules of a payment system must clearly specify potential participants and the requirements that need to be met to connect to the payment system, so as to present objective and non-discriminatory requirements for participation to potential participants and other interested parties in a transparent manner, without the restrictive factor of competition among the participants.

The operating rules of the payment system play a key role in helping participants understand financial risks they face. The efficient management of financial risks in the payment system requires that participants know the system characteristics and therefore understand their obligations and responsibilities regarding financial risk management. This means that the operating rules need to provide an in-depth and comprehensive framework of activities in the payment system, which means defining the entire flow of transfer orders execution – from submission and verification of electronic messages, acceptance, finality, rejection, calculating the net position of the participant (if netting is carried out in the payment system), setting the limit or another manner of securing settlement funds, until the settlement is performed.

The minimum requirement to be met to ensure protection from financial risk in the payment system is designing a payment system in such a way that the operating rules clearly determine the steps to be taken in all cases when a participant cannot settle its liabilities (e.g. rejecting the transfer order pertaining to the participant or re-calculating net position for other participants or other steps).

As the settlement agent is the necessary link in the transfer order execution, the operating rules need to clearly define the settlement agent and the steps to carry out the

[6] BIS – Central bank oversight of payment and settlement systems, 2005; Principles for Financial Market Infrastructures (PFMI), 2012; IMF – The Financial Sector Assessment Program (FSAP).

settlement procedure, in terms of crediting and approving the settlement account of the participant where funds used for settling liabilities and for the settlement between system participants are held. The operating rules or the contractual relationship need to precisely define the relationship between the operator and the settlement agent, as well as their roles and responsibilities, particularly in terms of the use of funds once the settlement is carried out.

The format and the purpose of electronic messages used in the payment system, the structure and elements of these messages and how they are exchanged between the participant and the operator, and between the operator and the settlement agent are of importance for the functioning of the system and need to be adequately addressed in the operating rules. This helps understand the standards to be used or adjusted for the format and the exchange of electronic messages and information on the functioning of payment system operations, and carrying out activities in the system. It is also significant for potential system participants so that they are able to review the access to the system in terms of necessary changes in their information systems.

The operating rules must include a daily time schedule of the payment system. It must clearly define working day periods when transfer orders are executed and messages exchanged with other participants. To manage risks, the operating rules may define cases allowing departures from the daily schedule of the payment system, and conditions and manner for approval of extending payment system's working hours at a participant's request. To adequately determine rights and obligations of operators and participants regarding risk management, the operating rules should determine the measures to be taken by the operator when the regular functioning of the payment system in hindered by unwanted or unexpected events (e.g. resuming payment system functionality from a back-up location and/or change of the daily time schedule), and the steps to be taken in case participants experience operational problems. Also, if the payment system allows indirect participation, the operating rules must clearly define such participation, as there are various types of indirect participation, as well as the ensuing rights and obligations.

The operating rules are one of the key documents that illustrate the payment system design – showing main characteristics of the system. Their significance lies in the fact that they establish the rights, obligations and responsibilities regarding the execution of transfer orders, and also in terms of risk management. If these rules are not clear, precise and comprehensive, there is a danger that participants may come under a false impression about security and reliability of the payment system, which may give an imprecise image of their risk exposure.

3 Trends in the European Union and activities of the Bank for International Settlements

Rapid technological development, new payment services and instruments, and efforts to improve the provision of these services on a global scale heated up the competitiveness in the payment services market, attracting new players who themselves provide these services and so create the need for a comprehensive and efficient protection of payment services consumers.

Over the last decade, ICT companies have largely shifted their operations towards the market of payment services and came to be its significant players, always offering innovative solutions. In some cases, activities of these entities are outside the scope of the standard technical services that support the provision of payment services (e.g. data processing, storage and protection, authenticity verification of data and agents, provision of services regarding IT and communications network, providing and maintaining the terminal and devices used for payment and related services). Their services therefore need to be adequately addressed by the regulatory framework. This primarily relates to payment instruments in case of a restricted network of vendors of goods and services, and within that context, of mobile phone apps, digital wallets, payment initiation services, account information services, virtual currencies and payment with these currencies etc. Likewise, the diversity of business payment models and their expected growth and development also pique the interest of all interest groups, regulatory bodies in particular. Creating the Single Euro Payments Area, EU regulatory bodies aim to ensure a harmonised legal framework across all EU member states, as well as the consistent use of payment instruments.

Developing new technologies, such as contactless payments (near-field communication), the use of tokens,[7] blockchain,[8] and other technologies, helps create new payment instruments, but also requires considering amendments to the regulatory framework. Most innovations were sparked by the actual needs of the market, and the overall market ambience and rules on payment services were amended owing to integration and standardisation of rules across the EU. This should reshape the regulations and practice at the national level and so affect how economic agents, financial and state institutions operate and how consumers use payment services. On the other hand, the global financial crisis created the need to improve risk management in the context of AML/FT and online payment security, and brought into focus the risks sparked by innovation and new technologies.

[7] Manual devices used for financial transactions authorisation.
[8] A complex infrastructure for execution of transactions by using a complex automated tech solution and the majority confirmation principle. Its best-known application is Bitcoin transactions execution.

Chart 2. Key objectives of regulatory activities in the EU

One of the key challenges of the EU supervisory bodies is the creation of a regulatory framework that will encourage competitiveness in the market and facilitate innovation. It should also provide unique rules to be applied to all players in the market, while preserving payment security and efficient risk management.

Having in mind the harmonisation of the Serbian legal framework on payment services with the relevant EU regulations, this report looks into activities, studies and analyses of the European Central Bank, central banks of EU member states, the Bank for International Settlements and other relevant institutions.[9]

In the 2013–2015 period, the ECB published a number of documents important for payment services market, including payment systems: Recommendations for the security of internet payments, Assessment guide for the security of internet payments, Guide for the assessment of credit transfer schemes against the oversight standards, Guide for the assessment of direct debit schemes against the oversight standards. The ECB also adopted a Regulation on oversight requirements for systemically important payment systems, and the related Assessment methodology for payment systems, as well as the Revised oversight framework for retail payment systems.

In 2015, the following key activities were carried out in the EU: adoption of a new directive regulating payment services in the internal market (Directive (EU) 2015/2366), publication of a document Eurosystem expectations for clearing infrastructures to support pan-European instant payments in euro and the Guide for the assessment of card payment schemes against the oversight standards.

[9] European Payments Council Blog and Discussion Board – EU Regulatory Initiatives Impacting the Security of EURO Payments: the 2015 Outlook; Eurosystem oversight policy framework, ECB, 2015; Eurosystem expectations for clearing infrastructures to support pan-European instant payments in euro, ECB, 2015; Guidance on cyber resilience for financial market infrastructures, BIS - CPMI-IOSCO, consultative paper, 2015.

The key activity of the Bank for International Settlements in 2015 was the publication of the Guidance on cyber resilience for financial market infrastructures – CPMI-IOSCO.[10] [11]

The ECB carries out supervision of these systems in line with the Regulation on oversight requirements for systemically important payment systems implementing the CPSS-IOSCO Principles for financial market infrastructures. In addition, through the revised oversight framework for retail payment systems, the ECB made a distinction between these payment systems so as to achieve adequate implementation of oversight requirements. The distinction was made based on whether these systems are systemically important for the EU (ESIRPS – European systemically important retail payment systems) or for the national markets (NSIRPS – National systemically important retail payment systems), and they are governed by the ECB decision. There are also payment systems not systemically important yet with an important role in ensuring security and efficiency of the financial system and preserving the confidence in the euro. As these have different risk profiles, the ECB classified them into two categories: PIRPS – Prominently important retail payment systems and ORPS – Other retail payment systems).

In addition to strengthening the security and stability of operation and transfer of funds between participants, retail payment systems oversight is also important as it: ensures public confidence that the use of specific payment instruments will create an adequate economic value (e.g. encouraging the use of e-payment instruments); efficiency – reducing cumulative payment fees proportionate to the scale of economic activity; effectiveness – encouraging swift and secure transfer of funds with the possibility of monitoring the transaction flow from start to end; the use of any payment instrument should result in equal costs, speed and security of payments when using these instruments, regardless of the location of the payer and payee.

Innovations, new payment services and the implementation of SEPA standards have changed the retail payment market, prompting the Eurosystem to apply a harmonised approach when overseeing payment instruments. This is done to ensure their security and efficiency and so preserve confidence in their use and consequently the currency itself. Altogether, this helps ensure the efficiency of the overall economy.

In terms of oversight, when payment instruments are governed by a payment scheme,[12] the key role is played by the entity that regulates the implementation of these rules, scheme participants' behaviour and the overall promotion of the payment instrument aimed at its widest possible use.

[10] Resilience to attacks and threats against information system resources (e.g. computer virus, worms, Trojan horses, Internet-based attacks etc.).
[11] Guidance on cyber resilience for financial market infrastructures – CPMI-IOSCO consultative paper, BIS, 2015.
[12] Unique rules on the manner of use of the instruments, and rights and obligations of all relevant participants. The rules are agreed on by payment service providers.

Managing the payment scheme, and thus the very payment instrument, primarily means managing risks to which the instrument is exposed, in particular legal, operational and financial risks, which can largely jeopardise users' confidence in the instrument. With this in mind, attention should be directed to the overall management of the payment scheme. Oversight standards used to assess payment scheme compliance were defined accordingly. To that end, in 2008 and 2009, the ECB published oversight policies for three key payment instruments in the EU: credit transfer, direct debit and payment cards. The guide for the assessment of card payment and credit transfer schemes against the oversight standards were published in 2014, while the Guide for the assessment of direct debit schemes against the oversight standards was published in 2015.

Table 1. Payment instruments oversight standards in the EU

Standard I	The governance authority should establish rules and contractual arrangements for governing the payment instrument scheme in such a way that they provide a complete, unambiguous and enforceable legal framework for the proper functioning of the scheme. The rules and contractual arrangements should be compliant, in all circumstances, with applicable national and EU legislation.
Standard II	The scheme should ensure that comprehensive information, including appropriate information on financial risks, is available for all actors. Clear, comprehensive and up-to-date documentation is essential for the smooth functioning of a payment instrument scheme. This documentation should be readily available in order to enable all actors to take appropriate action in all circumstances. In particular, actors should have access to relevant information in order to enable them to evaluate and mitigate financial risks; this will reduce the risk of a loss of confidence in the payment instrument through unexpected financial losses, including fraud. However, sensitive information should only be disclosed to the relevant actors on a need-to-know basis.
Standard III	The scheme should ensure an adequate degree of security, operational reliability and business continuity. Operational risks, including fraud, could have a serious impact on the schemes offering the payment instrument. Operational risk results from inadequate and/or the failure of internal processes and systems as a result of human error or external events. This could lead to a financial loss for one or more of the parties using the payment instrument, thereby undermining the users' confidence in it. Thus, adequate security controls should be in place to mitigate operational risks. In this regard, the governance authority should ensure that all relevant actors in the scheme focus on risk and security management, business

	continuity and outsourcing by ensuring that adequate technical standards and procedures are in place.
Standard IV	The scheme should implement effective, accountable and transparent governance arrangements. Efficient decision-making bodies and processes are needed in order to prevent, detect and respond promptly to disruptions. Effective internal control processes are also essential in order to prevent any loss of confidence in the scheme.
Standard V	The governance authority of the scheme operating a payment instrument should ensure that clearing and settlement providers are fit to perform their role in the scheme by identifying the financial risks involved in this process and by having the appropriate measure defined in order to address these risks. Any procedures to complete settlement in the event of default should not undermine the solvency of the actors committing resources to complete settlement, and payment system participants need to be fully aware of their responsibilities ensuing from these procedures.

In terms of payment security, another important body in the EU/EEA payment services market is the European Forum on the Security of Retail Payments – SecuRe Pay, which is a common platform of the European Central Bank and the European Banking Authority (EBA). Its main focus is on the security of electronic retail payment services, systems and schemes. SecuRe Pay also encourages cooperation between authorities and thus supports the establishment of harmonised policies and regulations in this field (e.g. guidelines, technical standards, oversight framework). Working to improve the security of the provision of payment services, the Forum analysed the security issues of payment initiation services and account information services. Following the analyses, in 2014, SecuRe Pay published a set of recommendations that complement recommendations for the security of internet payments. Building on the Forum's recommendations, a new directive on payment services in the internal market (Directive (EU) 2015/2366) included also payment initiation and account information services. Among other, the EBA is entrusted a leading role in respect of drafting regulatory technical standards for payment service providers. The standards should aim to ensure an appropriate level of security for payment service users and payment service providers, the safety of payment service users' funds and personal data, technology and business-model neutrality, and allow for the development of user-friendly, accessible and innovative means of payment. In terms of payment systems infrastructure, the new Directive has changed the provisions on payment system access. To ensure fair competition between payment service providers, a participant in

a designated payment system, determined as important under Directive 98/26/EC, which provides services in relation to such a system to an authorised or registered payment service provider should also, when requested to do so, grant access to such services in an objective, proportionate and non-discriminatory manner to any other authorised or registered payment service provider.

In line with innovations in the payment services market, the Euro Retail Payments Board (ERPB)[13] launched an initiative and invited the European Payments Council (EPC) – a body that represents payment service providers in Europe – to develop a scheme for instant payment in euro. In order to foster a single instant payment market, the Eurosystem expects payment systems to adopt a pan-European approach to reach this goal and adequately manage risk. To achieve this, the ECB published a set of expectations for clearing infrastructures to support instant payments in a single market. Instant payment is defined as "electronic retail payment solutions available 24/7/365 and resulting in the immediate or close-to-immediate interbank clearing of the transaction and crediting of the payee's account with confirmation to the payer (within seconds of payment initiation)."

Given the specificities and significance of the pan-European market for payments in euro – which basically translates to equalling national and cross-border transactions – it is emphasised that under the instant payment scheme, payment service providers need to be available to each other and that payment systems need to bear this availability in mind. When DNS technology is applied to transfer funds between different payment service providers, for instant payments to function it is of key importance that payee's PSP (payment service provider) makes the funds available to the payee before receiving them from the payer's PSP. The scheme itself can contribute to credit risk management by setting a maximum amount limit for individual instant payment transactions. Also, infrastructures are expected to put in place appropriate risk management mechanisms, primarily regarding credit risk (e.g. pre-funding, cash guarantee funds and/or securities guarantee funds). The ECB underlines that in an ideal case, risk management measures should be harmonised in payment systems to ensure cross-border interoperability. The Eurosystem has called on market participants to define requirements for settling instant payments and the related risk mitigation. As a market infrastructure operator, the Eurosystem will take such requirements into consideration to support the settlement of instant payments in TARGET2.

As financial market infrastructures, including payment systems, play an important role in promoting financial system stability, one of the key activities of BIS in 2015 was publication of a set of guidelines on cyber resilience of the financial market infrastructure. This was done as operational resilience, including cyber resilience, of these infrastructures may be decisive in the overall resilience of the financial system.

[13] The ERPB was launched in 2013 to help foster the development of an integrated, innovative and competitive market for retail payments in euro in the European Union. It is chaired by the ECB and consists of representatives of payment service providers, consumers and member states central banks.

BIS published a set of guidelines to improve cyber resilience of infrastructures, guided by the dynamic nature of cyber threats and the importance of interconnectedness of related entities. These guidelines also define some of the challenges that cyber risks pose to the traditional frameworks for managing operational risk of infrastructures (e.g. need for a swift and safe contingency plan following a cyber-attack). The document elaborates on the established Principles for Financial Market Infrastructure, without introducing any standards.