NATIONAL BANK OF SERBIA

PAYMENT SYSTEM DEPARTMENT

PAYMENT SYSTEM OVERSIGHT

Second half of 2016

Contents:

Introduction

The National Bank of Serbia (NBS) supervises/oversees payment systems in accordance with the Law on the National Bank of Serbia, Law on Payment Services and regulations adopted under that Law, governed by the principles of transparency, application of internationally recognised standards for the operation of payment systems and consistency in the application of requirements and standards to comparable payment systems.

It is primarily the payment systems themselves that fall within the scope of oversight/supervision, while oversight/supervision activities focus on the operation of the system as a whole, rather than on the individual participants.

On the other hand, payment instruments also fall within the scope of oversight, and their usage initiates payment transactions executed in the payment systems – if the use of those instruments is governed by special rules agreed between the issuers. Payment instrument oversight is an important part of payment system oversight where payment transactions initiated by those instruments are executed and includes primarily consideration of the security of their use which is relevant for maintaining public trust in the national currency.

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

1. Market participants

Acting upon applications for licences for payment system operation, the NBS verifies compliance with the requirements prescribed by the Law on Payment Services and bylaws adopted under that Law, pertaining to organisational, personnel, technical and other conditions, management and internal control system and payment system risk management. As a result of conducted actions, the NBS resolved positively two applications and at end-2016 passed a decision on issuing a licence to the Association of Serbian Banks, p.u. for payment systems operation – ASB clearing of cheques and ASB clearing of direct debits, and one payment system operation licence application was rejected as it was determined that not all the requirements were met.

At end-2016 two payment system operators operated in the Republic of Serbia – the NBS managing four payment systems (NBS RTGS system, NBS clearing system, NBS interbank clearing of foreign exchange payments system and DinaCard clearing system) and the Association of Serbian of Banks p.u. managing two payment systems (ASB clearing of cheques and ASB clearing of direct debits). Payment systems, for which the Association of Serbian Banks p.u. is licenced in accordance with the Law on Payment Services, had operated even before this Law entered into force in accordance with the provisions of the Law on Payment Transactions and regulations passed under that Law.

Table 1 provides an overview of the listed payment systems, types of transfer orders executed in those systems and the manner in which settlement based on those orders is performed.

The NBS RTGS system and NBS clearing system were established as important payment systems in line with the regulations – systems of significance for the stability of the financial system, and, in addition to requirements prescribed for all payment systems, they are also subject to the provisions of the Law on Payment Services governing the finality of settlements in an important payment system, as well as additional requirements stipulated by bylaws. This particularly refers to defining the moment of transfer order acceptance in the system and the moment when a participant and the third party cannot revoke that order (the moment of irrevocability) – which is significant for the reduction of legal and systemic risks in executing transactions in an important payment system. In addition, one of the requirements is for the operator of an important payment system to undertake all reasonable measures to ensure the continuation of key business processes related to the work of an important payment system at the latest two hours after the occurrence of an event disabling the regular operation of that system, that is, all reasonable measures to ensure the completion of the settlement based on transfer orders at the latest by the end of the day when the settlement must be performed.

Table 1 Overview of payment systems in the Republic of Serbia

Payment system name	Transfer orders executed in payment system	Settlement method
NBS RTGS	Orders based on credit transfers whereby participants initiate transfer of funds, in their name and for their account, as well as for purpose of executing payment transactions of their payment service consumers; orders for executing payment transactions aimed at implementing the NBS monetary policy; orders for the settlement of financial liabilities, that is, receivables created in other payment systems and systems for the settlement of financial instruments; orders originating from supplying banks with cash and taking over cash from banks in line with the NBS regulations; other orders in line with the system operational rules	Real-time gross settlement principle
NBS clearing	Orders based on credit transfers whereby participants initiate transfer of funds, in their name and for their account, as well as for purpose of executing payment transactions of their payment service consumers, in individual amount of RSD 300,000.00	Designated-time net settlement principle
NBS interbank of foreign exchange payments	Orders based on credit transfers in euros in the Republic of Serbia, pursuant to the regulations	Designated-time net settlement principle
NBS DinaCard clearing	Orders originating from payment transactions performed using DinaCard payment cards	Designated-time net settlement principle
ASB clearing of cheques	Orders originating from payment transactions performed using cheques	Designated-time net settlement principle
ASB clearing of direct debits	Orders originating from payment transactions with direct debits of ASB, in terms of the Law on Payment Services, in individual amount of RSD 300,000.00.	Designated-time net settlement principle

With the exception of the NBS RTGS system where transfer orders are executed on real-time gross settlement principle, transfer orders in all other systems are executed on designated-time net settlement principle, i.e. settlement is performed of net positions occurring as a result of netting based on transfer orders in these systems in terms of the Law on Payment Services, in line with the operational rules of those systems and the NBS RTGS system.

In addition to being the payment system operator, the NBS is simultaneously the regulator of payment systems, has the role of a settlement agent, and on the other hand supervises/oversees payment systems and issues and revokes licences to payment system operators. Such a specific position of a central bank in the payment system market is not unique to the Republic of Serbia. Central banks of all the EU member states are the operators of the TARGET2 components, and individual national central

banks are also the operators of the Retail Payment Systems[1]. The supervision/oversight task is shared between the European Central Bank and national central banks of the EU member states, depending on the importance of the payment system – the European Central Bank has a lead role in the supervision/oversight of the TARGET2 components, and other payment systems systemically important for the EU market. On the other hand, the European Central Bank and national central banks are also the regulators of the payment system market.

All of the above roles of central banks developed as a response to changes which occurred in the payment system area – payment systems gained in importance due to an increasing number and value of executed transactions and new technical and technological solutions, but also as a result of the incapacity of entities in the market to arrive at solutions that would ensure smooth operation of a payment system, that is, that would respond to the needs of the economy. Central banks have also recognised their role in the global current affairs related to the fast payments, the so called instant payments. Majority of central banks consider the implementation of instant payments a strategic option in the area of payment systems aimed at modernising the national infrastructure, creating the basis for the development of innovative solutions in the area of payment instruments, enhancing payment speed, ensuring a unique solution and promoting financial inclusion.[2] According to a BIS study[3] the level of support and access to be accepted by central banks in the area of instant payments development comprises different scenarios.[4]

Bearing the above in mind, what is particularly important in the area of supervision /oversight is consistency in the application of requirements and standards to comparable payment systems.

2. Regulatory framework

The previous report reviewed aspects of the payment system regulatory framework with regard to activities carried out in the payment system, specificities of risk which can occur and the significance of rules of the payment system.

In order to give a complete picture, substantially this report puts stress on the management and internal control systems. Pursuant to the regulations governing the payment system operation, an operator shall establish, maintain, and upgrade reliable, efficient and comprehensive management and internal control systems which ensure

[1] E.g. Banca d'Italia – Bi-Comp, CABI clearing system, Bank of Lithuania – SEPA MMS, Deutsche Bundesbank – RPS, Bank of Greece – ACO, Banco de Portugal – SICOI.
[2] Fast payments – Enhancing the speed and availability of retail payments, BIS, 2016.
[3] Ibid.
[4] Scenarios presented in the BIS study with examples: "Business as usual" – Italy, India, "Moderate support" – Sweden "24/7 RTGS or special settlement services" – Australia, "Central bank as fast payment system operator" – Mexico.

stable, secure, efficient and effective payment system operation and responsible and reliable management of the system operation. Clearly, these systems are primarily established for the risk management purpose and are considered reliable, efficient and comprehensive if enabling the operator to manage risks to which the payment system operation is exposed or could be exposed, including when the operator entrusted certain operational tasks to another party.

The operator's management system is based on the relations between different entities in the interest of which is for the payment system to operate. Considering that this system provides to the operator the basis for setting the goals concerning the payment system operation, determining the manner for the achievement of those goals and monitoring of the achievement[5] – the management system must be considered directly in relation to other requirements prescribed for the operation of payment systems.

The Law on Payment Services stipulates the legal form for entities which can be payment system operators, and hence differences in the manner of establishing the payment system management are possible.

What is important for this system is to precisely and clearly establish (document), in a transparent and consistent manner job distribution and division, as well as duties and responsibilities regarding the operation of the payment system and risk management in the payment system, in the organisational structure of the operator in such a way to avoid the conflict of interests. This implies that the operator should clearly define in its internal acts the division of duties and responsibilities between the managing bodies, payment system manager and other operator's employees – concerning the operation of the payment system and management of financial, operational and other risks to which this system is exposed or may be exposed. Also, the scope of work of every operator's organisational unit relevant for the payment system operation and risk management in this system needs to be clearly defined with clear lines of responsibility. In addition, the management system will enable to the operator to manage risks in the payment system adequately if:

- Risk management and internal audit independence are ensured, including their authority and access to managing bodies;
- There is effective communication and cooperation at all organisational levels that were assigned certain responsibilities regarding the operation of the payment system and risk management in this system and the information flow is adequate i.e. if relevant information is disseminated efficiently at horizontal level, and particularly at vertical level;
- Clear and documented decision making process is ensured regarding the operation of the payment system and risk management in this system.

[5] Principles for financial market infrastructures – CPSS-IOSCO, BIS, 2012.

With the internal control system an operator takes care of prevention of excessive risk exposure, ensures operation compliance with the regulations and may prevent, that is, eliminate different irregularities. As the name says, internal controls are established in the operator's internal operations and comprise different business segments. Controls with regard to ensuring operator's compliance with the regulations, but also with the operational rules of the managed payment system and internal acts are particularly important for the payment system operation. Controls of implementation of procedures and establishment of irregularities in their implementation, ensuring validity of data and information in the reports, timely and accurate publishing of information on the payment system in line with the regulations, physical and logical control of access to the information system, and verification of adequacy of the information system for the nature, volume and complexity of operations in the payment system are also significant. In addition to the above, the operator should also protect the interests of payment system participants in the managed system using the internal control system.

Bearing in mind that internal controls need to be a part of everyday activities of every operator's employee, by implementing them they provide a significant contribution to internal control system upgrade through timely observation of potential deficiencies and timely vertical information dissemination, which is why control environment and management support are also important.

Operator's internal audit is important because it ensures independent and comprehensive assessment of the adequacy of the payment system management system, and particularly the internal control system and the risk management in a payment system.

In addition to key objectives of stability and security, the operation of the payment system should be efficient and effective, particularly in the area of the participants' needs, in which case the operator should actively cooperate with the participants and potential participants (consultations with participants but also possibly market analysis, the analyses of technical and technological solutions, of system utilisation costs and alike). If a payment system is not efficient and effective, it can jeopardise financial activity and expose its participants and their clients to risks.

3. Overview of developments in payment system oversight – the Bank for International Settlements and the European Union

3.1. The Bank for International Settlements – Guidance on cyber resilience for financial market infrastructures[6]

Attempting to live up to expectations of financial service consumers and offer as wide as possible a range of easily accessible products and services, the financial sector expresses increasing requests for the speed of product delivery and execution of financial transactions. Hence, investment in new technology is the pillar of competitive advantage which enables support to market requirements. However, concurrently with the development of new technology and digitalisation of financial services, cybercrime is also developing and the risk of cyber threats and attacks is increasing (social engineering, skimming, phishing, identity fraud, hacking, ransomware).

According to the OECD Report for G7[7], the number of cyber incidents and companies affected significantly rose. Hence, the World Economic Forum identified in its 2017 Global Risks Report the cyber risk as one of the most significant risks faced by companies in five G7 countries. The OECD recognised that globally countries largely adopted national strategies for IT security which should raise awareness of risk management in digital business, without treating the cyber security as the issue of economic and general social risk management.

Following the trends in both directions (security and financial innovation), international regulatory bodies focused their attention on creating conditions for as secure as possible business environment, for all participants in the payment chain, and as result a series of activities were undertaken and specific measures and acts adopted, governing the area of IT security in general for payment services and hence for payment systems supporting those services.

As financial market infrastructures, including payment systems, have an important role in promoting the financial system stability, in 2016 the Bank for International Settlements (BIS) published Guidance on cyber resilience for financial market infrastructures (hereinafter: Guidance). In this Guidance cyber resilience is defined as "the ability of an organisation to anticipate, withstand, contain and rapidly recover the financial market infrastructure from a cyber attack". Therefore, according to BIS, cyber resilience, in terms of operational reliability of the financial infrastructure operation, serves for the achievement of objectives of financial stability which is why

[6] "Guidance on cyber resilience for financial market infrastructures", Committee on Payments and Market Infrastructures, Bank for International Settlements, June 2016. http://www.bis.org/cpmi/publ/d146.pdf.
[7] "Supporting an effective cyber insurance market", OECD, May 2017.

consistency in supervision/oversight of infrastructures and their participants by different competent bodies is important.

Governed by principal objectives aimed at achieving the greatest possible degree of security and efficiency of financial infrastructure which contains the systemic risk, BIS recognised the cyber risk as the key risk among operational risks faced by all financial infrastructures today. BIS sees this risk as a unique challenge imposed on traditional frameworks for operational risk management in infrastructure considering the specific features which distinguish it from other types of operational risks, reflected in the following:

- Cyber attacks are difficult to anticipate, identify, estimate the exact degree of loss and eradicate them completely. They are often imperceptible and spread with high speed within the system network;
- Cyber attacks may come from different entry points in infrastructure of financial market because of the presence of interdependent entities in the chain of payment execution, related entities, providers of technical services that support the work of infrastructure, but even employees may be the entry point;
- Cyber attacks significantly account for inefficiency of the risk management system and business continuity.

Bearing in mind the above specific features of cyber risks, BIS is of the opinion that it is necessary to establish a comprehensive framework for operational risk management which will cover cyber risk as well, by defining a clear strategy and objectives of cyber resilience.

The framework for managing cyber resilience set in the Guidance is composed of five key stages (Governance – Identification – Protection – Detection – Response and Recovery) and three components common to all five stages (Testing – Situational awareness – Learning and evolving).

- Governance

An efficient cyber risk management system is considered substantially important for a systemic and proactive approach to managing current and emerging threats faced by certain infrastructures. A management system needs to cover all the levels of one organisation and ensure appropriate resources and the expertise of staff addressing this risk. This is why efficient cyber resilience governance means defining, primarily, clear and comprehensive framework which includes ICT equipment, manpower, processes and requests imposed by new technologies, as well as timely communication with all stakeholders in order to ensure efficient response to, and recovery from a cyber attack. In addition, the framework needs also to be adjusted with the defined strategy for cyber resilience and objectives to be met for that purpose.

- Identification

Occurrence of each type of operational risks in the financial market infrastructures may potentially jeopardise the financial stability, and hence the identification and classification of all crucial business processes, information assets and external entities on whose operations certain financial market infrastructures depend is very important for efficient management of cyber resilience, which will be the priority in protection against compromise.

- Protection

Security and internal control systems and processes need to be designed in such a way to protect the confidentiality, integrity and availability of financial market infrastructure information system. Controls need to be proportionate to the role of a certain infrastructure in the financial system and threats to which it is exposed, with adequately defined risk tolerance.

- Detection

The ability to recognise early signs of a potential cyber attack, or detect as early as possible that an actual system breach has taken place is essential to the framework for managing cyber resilience. Early detection of fraudulent activities provides for proactive actions aimed at preventing system breaches or mitigating the impact through disabling access to confidential information and their export. Hence, Guidance points out to the significance of an efficient system for continuous monitoring of unusual actions and defining necessary activities in case of incident.

- Response and Recovery

At this stage of cyber resilience management, the stress is on the development of the ability of adequate response and taking measures for system recovery from a cyber attack. In that sense, what needs to be ensured is for key functions to be established in a fast and secure way, and with precise information in order to alleviate the potential systemic risk. Hence, well defined incident response plans, continuity plans, and system recovery plans are of paramount importance.

Bearing the above stages in mind, Guidance indicates the significance of testing each of the elements of the system for managing cyber resilience before employing them within the financial market infrastructure, in order to estimate its total efficiency and to monitor it during regular operation of infrastructure. Reliable and detailed testing contributes to the identification of deficiencies of the defined goals of cyber resilience and provides credible and significant data necessary for the process of managing this risk. On the other hand, the analysis of data obtained through testing proactively leads to the manner in which discovered weaknesses and deficiencies can be corrected, reduced or entirely eliminated. In addition to testing, what is also important is awareness and regular monitoring of the situation in the surrounding area

concerning the potential cyber threats, as well as potential consequences of the infrastructure operation in such environment. In order to raise awareness on cyber threats it is very important to establish an efficient system of information dissemination to enable timely and fast reaction to prevent cyber attacks or detect them as soon as possible. Hence, active participation in information sharing is indispensable, as well as cooperation with all the stakeholders, not only in the area of financial infrastructure operation, but also in the wider range of entities. It is also necessary to provide for continuous development and engagement of staff on finding adequate solutions for adjustment to the dynamic nature of cyber risks, and on the development of ability for timely identification, assessment and management of threats and detection of system weak points.

Guidance also indicates that an organisation governing the financial market infrastructure needs to implement organisational cyber culture that particularly includes raising awareness on this risk and continuous staff knowledge and competence development in this area.

3.2. Instant payments

According to the Euro Retail Payments Board (ERPB), instant payments are a solution to electronic retail payments available to payment service consumers in the 24/7/365 mode resulting in a current or almost-immediate credit to payee's account.[8] Namely, transition of operation to electronic mode, particularly electronic commerce and use of digital communications conditioned the payment service consumers to expect solutions at their disposal which will enable them fast payments.

Use of smart phones and integration of sale channels open 365/24/7 by a merchant, together created conditions for a consumer to be able to execute payments at any time and from any point, and not only person-to-business transactions but also person-to-person transactions. Potentials of market and technological innovations should be supported, which is a result of the adoption of SCT Inst scheme in the EU.[9] When preparing the above scheme, the European Payments Council took into account the business requirements, which, among other things, related to: the availability of instant payments service for payment service consumers, the availability of funds for payee, understanding of the concept of executing instant payments within "a few seconds" by all participants, establishment of a reliable system for identification of payment service consumers to avoid errors, establishment of standardised financial and non-financial messages and alike. Instant payments open space for competition in the area of instruments whereby non-cash payments may be initiated and use of the

[8] Pan-European instant payments in euro: definition, vision and way forward, ERPB, 2014.
[9] European Payments Council (EPC) adopted a SCT Inst Scheme for the European single Payments Market.

potential for mobile payments, all of which should contribute to a further development of e-commerce.

In view of the fact that at end-November 2016 SCT Inst scheme was adopted, in the same period the Euro system carried out a series of activities focusing on the analysis of the market needs for services of instant payment settlement in the 24/7/365 mode.

A special task force headed by the representatives of the European Central Bank prepared a specification of consumer requests for new services of TARGET instant payments. The above initiative is a result of the objective of the Euro system to respond to growing demand for instant payments in the European market and to avoid national solutions which would lead to market fragmentation instead of providing a single market.

Recognising that these are important innovations in the retail payments market, as a result of a conducted research, in November 2016 the BIS published a study "Fast payments – Enhancing the speed and availability of retail payments.[10]

From the perspective of supervision/oversight of payments system operation, the introduction of instant payments may have a positive effect on efficiency. However, if safe and stable operation of payment systems for instant payments is considered, though the risks to which payment systems are exposed are the same, they gain a new dimension in the conditions of 24/7/365 mode and under the rule that payee's payment service provider must put funds at payee's disposal in advance, without having received the funds from the payer's payment service provider.

Central banks' approach to supervision/oversight of payment systems for instant payments may differ from country to country bearing in mind the application of the Principles for the financial market infrastructure primarily intended for systemically important payment systems. Considering that most of the instant payment systems will not be systemically important – differences may arise in oversight policies which is an aspect that will gain in importance in the coming years, in terms of achieving a certain degree of standardisation globally.

[10] Fast payments – Enhancing the speed and availability of retail payments, BIS, 2016.