Pursuant to Article 156, paragraph 5 and Article 176, paragraph 4 of the Law on Payment Services (RS Official Gazette No 139/2014) and Article 59, paragraph 2 of the Law on the National Bank of Serbia (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), the Governor of the National Bank of Serbia issues the following

D E C I S I O N
ON THE MANNER OF MAINTAINING AND ENHANCING SAFE AND SOUND PAYMENT SYSTEM OPERATION AND REPORTING TO THE NATIONAL BANK OF SERBIA

Title I

INTRODUCTORY PROVISIONS

1. This Decision sets out in detail the manner of maintaining and enhancing safe and sound payment system operation, as well as the elements of data on the operation of payment systems which the operator delivers to the National Bank of Serbia (hereinafter: NBS) under Article 176 of the Law on Payment Services (hereinafter: the Law) and the deadlines and manner of delivery of such data.

2. The provisions hereof shall apply to the part of the operator's operations relating to management of payment system operation, including the performance of activities in that system.

Title II

MANNER OF MAINTAINING AND ENHANCING SAFE AND SOUND PAYMENT SYSTEM OPERATION

3. A payment system operator (hereinafter: operator) shall at all times maintain and enhance safe and sound payment system operation and shall especially ensure the following:

1) fulfilment of organisational, personnel, technical and other requirements established by the Law and this Decision;

2) proper governance and internal controls systems;

3) management of financial, operational and other payment system risks (hereinafter: risks).

Chapter 1

ORGANISATIONAL, PERSONNEL AND TECHNICAL REQUIREMENTS

4. The operator shall have appropriate organisational, personnel and technical capacity for the performance of activities relating to payment system operation, proportionate to the nature, complexity and scope of such activities.

5. Organisational capacity of the operator shall mean:

1) appropriate organisation of activities relating to payment system operation, and/or such organisational structure that ensures smooth performance of such activities within one or several organisational units;

2) business premises where activities relating to payment system operation are performed, which have to be in the ownership of the operator or rented or leased for a period of at least three years and which meet legal requirements relating to technical capacity, work safety and environmental protection.

6. Personnel capacity of the operator shall mean the number of employees sufficient to carry out activities relating to payment system operation, efficient functioning of the governance and internal controls systems and risk management, possessing professional qualifications and experience adequate for their duties, responsibilities and the complexity of activities they carry out.

7. Technical capacity of the operator shall mean the provision of hardware (computer and communications equipment, media for data storage and other technical equipment supporting payment system operation) and software (system and application software required for payment system operation) whose capacity, functionality and characteristics are adequate for the nature, scope and complexity of activities in the payment system.

Chapter 2

GOVERNANCE AND INTERNAL CONTROLS SYSTEMS

8. The operator is obligated to establish, maintain and enhance reliable, efficient and comprehensive governance and internal controls systems that provide for safe, sound, efficient and effective payment system operation and responsible and reliable management of the system's operation.

9. For the purposes of this Decision, the governance system shall in particular include the following interconnected elements:

1) organisational structure of the operator, with precisely and clearly defined, transparent and consistent division and separation of activities, and duties and responsibilities relating to payment system operation and risk management in such system, established in such a manner as to prevent conflict of interest;
2) system for managing risks in the payment system;
3) internal controls system;
4) appropriate cooperation with payment system participants (hereinafter: participants).

10. The organisational structure of the operator should:

1) enable effective communication and cooperation across all organisational levels, including an appropriate horizontal and, particularly, vertical flow of information, in order to enable access to information which is significant for the process of decision-making regarding payment system operation and risk management in such system, and/or for the exercise of employees' duties and responsibilities.

2) ensure a clear and documented decision-making process regarding payment system operation and risk management in the system.

11. For the purposes of making decisions on payment system operation, the operator is obliged to establish regular reporting on such operation.

12. Within the meaning of this Decision, the system for managing risks in the payment system shall include risk management policies and process as well as reporting on risks, which enable the operator to manage risks to which payment system operation is or could be exposed.

The risk management system shall be established in accordance with this Decision, as well as with good business practices and generally accepted standards in this area.

13. The operator is obliged to adopt a policy that will regulate risk management, particularly management of financial and operational risks.

The policy referred to in paragraph 1 hereof shall mean one or more documents that contain in particular the main goals and principles of risk management, as well as the roles and responsibilities for risk management.

14. The operator is obliged to set up an effective and efficient risk management process which shall include procedures, processes and actions enabling comprehensive and timely identification, analysis and evaluation of risk (risk assessment), risk handling and monitoring.

The operator shall keep records on possible sources of risks (threats), identified risks and their analysis and assessment, and shall establish a register of risks in that regard.

The operator is obliged to carry out risk assessment at least once a year or more frequently, if necessary.

15. For the purposes of making decisions on risk handling measures and monitoring the results of such measures' implementation, the operator is obliged to establish regular reporting on risk exposure and provide extraordinary reports in the event of unexpected significant risk exposure.

The operator is obliged to timely provide to participants correct and complete data and information necessary for the management of risks to which participants are exposed in the payment system.

16. The operator shall review and if necessary, change the risk management system.

17. The operator shall designate key employees tasked with risk management and ensure their replacement so as to prevent their absence from work or termination of employment from disrupting safe and sound payment system operation.

18. For the purposes of this Decision, the internal controls system shall mean appropriate procedures, processes and actions adopted and/or undertaken in order to prevent excessive risk exposure of the operator and the payment system, as well as irregularities and illegalities in the operations

of the operator and/or the payment system, and to protect the interest of participants.

19. The operator is obliged to draw up procedures for all business processes relating to payment system operation, which shall be adequately detailed and descriptive, in proportion to the nature, scope and complexity of activities in the payment system.

The procedures shall in particular contain the description of the business process and the place where such process is carried out, description of activities within the business process and definition of employees' duties and responsibilities for the performance of such activities, as well as responsibilities for making decisions and implementing procedures.

The procedures shall be updated and harmonised with the business processes to which they relate.

Employees shall be informed about the content of the procedures necessary for the performance of their activities.

20. Within the internal controls system, the operator shall establish efficient and effective control activities that shall in particular relate to:

1) control of implementation of procedures and identification of irregularities in the course of their implementation;
2) assessment of whether data and information are correct and identification of possible deficiencies and errors in the reports stipulated by this Decision;
3) verification of compliance of the operator's activities with regulations, payment system rules and the operator's acts;
4) determining whether information and data on the payment system are timely and appropriately disclosed as stipulated by the Law;
5) physical and logical controls of access to the information system;
6) verification of whether the information system is adequate for the nature, scope and complexity of activities in the payment system.

The operator shall ensure that internal controls are a part of everyday activities of all employees, and that, in accordance with ethical and professional standards, employees understand the purpose and significance of these controls and their contribution to the implementation and enhancement of these controls.

21. In making decisions regarding payment system operation and management of risks in the system, and in particular when making decisions relating to payment system rules, the operator shall cooperate with participants in an adequate manner (e.g. consultations with participants, forming bodies in which participants shall have their representatives etc.).

20. As regards the assessment of adequacy of the governance system, the operator is obliged to ensure that internal audit carries out independent, regular and comprehensive review and assessment of the system.

Chapter 3

PAYMENT SYSTEM RISK MANAGEMENT

Minimum requirements for financial risk management

23. Financial risk in the payment system is the possibility of occurrence of negative effects on payment system operation due to the inability of a participant or another person in the system to meet its due obligations (liquidity risk), and/or to permanently fulfil its obligations (solvency risk).

24. In its payment system rules, the operator is obliged to clearly, precisely and comprehensively determine the manner in which processing of transfer orders, netting and settlement set forth by the Law are performed, so that financial risk in the system is clearly identified.

If the processing of transfer orders and netting in respect of such orders (clearing) are performed in the payment system, the operator is obliged, in its payment system rules, to determine the manner of acting in the event of a participant's inability to settle its financial obligation in respect of its net position at the moment when it is expected to do so, and to establish adequate procedures in line therewith.

In determining the manner of acting in the case referred to in paragraph 2 hereof, the operator shall take into account the degree of payment system exposure to financial risk and whether such system was determined as important in accordance with the Law and regulations adopted based on that law (hereinafter: important payment system).

25. To manage financial risk adequately, in its payment system rules the operator is obliged to determine the manner of acting in the event of a participant's inability to settle its obligations due to the issuance of a relevant decision on license revocation and/or an act passed by a relevant body to open bankruptcy proceedings or undertake other measures, in accordance with law, intended to wind up or reorganise the participant and involving the imposition of a ban on the disposal of funds in the participant's account, and to establish adequate procedures in that regard.

26. If a given bank is a settlement agent for a payment system and does not act as the operator of the system at the same time, the operator is obliged to regularly assess, monitor and handle the financial risk to which system operation is exposed because of the choice of such bank as the settlement agent.

27. The operator is obliged to regulate in detail the rights and responsibilities of the operator and the settlement agent regarding settlement activities, through a contract and/or system rules, particularly with regard to disposal of funds after the settlement.

Minimum requirements for operational risk management

28. Operational risk in the payment system is the possibility of occurrence of negative effects on payment system operation due to failures by employees, deficiencies in the work of information and other systems, inadequate internal procedures and processes, and due to the occurrence of unpredictable external events.

29. In accordance with the nature, scope and complexity of activities in the payment system, the operator is obliged to set up an adequate information system for collection, storage, processing, transfer, keeping, presentation and use of data and information.

For the purposes of this Decision, the information system shall mean a set of the following interconnected elements:

1) hardware and software referred to in Section 7 hereof;
2) information assets – data in files and databases, technical documentation, user guides, plans, procedures etc.;
3) information system users – all persons authorised to use the information system (employees in the operator, employees in a participant and other entities that have been given access to the information system).

For the purposes of this Decision, the information system elements referred to in paragraph 2, provisions 1) and 2) hereof shall mean information system resources.

30. The operator shall ensure that generally accepted standards for the format and exchange of electronic messages are used or adjusted for the performance of activities in the payment system.

31. In order to manage operational risk in the payment system adequately, the operator is obliged to determine minimum operational/technical requirements for participation in such a system.

32. In its payment system rules, the operator shall determine the manner of acting in the event of operational problems of participants and establish appropriate procedures in this regard.

Information system security

33. The operator is obliged to ensure security of the information system referred to in Section 29 hereof, in particular the security of such system's resources, and to adopt, in accordance with its complexity, the information system security policy taking into account good business practices and generally accepted standards in this area as well.

34. For the purposes of this Decision, information system security shall mean upholding the principles of:

1) confidentiality – ensuring that data and information are available to authorised persons only;
2) integrity – protection of accuracy and completeness of data and information;
3) availability – ensuring that data and information are available and usable upon the request of authorised persons;
4) authenticity – ensuring that the identity of participants or other persons relevant for the functioning of the payment system is as claimed;
5) non-repudiation – ensuring that an activity performed in the information system or receipt of information cannot be denied;
6) reliability – ensuring that the information system consistently and predictably performs the expected functions and provides correct data and information;

7) accountability – ensuring that each activity in the information system may be traced uniquely to its source.

35. The information system security policy shall mean one or more documents that shall in particular define the goals and key principles of achieving and maintaining an adequate level of information system security, including authorisations and responsibilities relating to such security and system resources.

36. The operator is obliged to harmonise the information system security policy with any changes in the business environment and in the very information system.

37. The operator shall ensure that the electronic message referred to in Section 30 of this Decision meets the requirements set forth by Section 34, provisions 1), 2), 4), 5) and 7) hereof.

Payment system operational reliability

38. With a view to assessing efficiency and effectiveness of payment system operation, the operator is obliged to define objectives of operational reliability and ways for their attainment, and to regularly monitor and assess whether payment system operation is consistent with these objectives.

Objectives of operational reliability shall include quantitative and/or qualitative indicators of the level of quality of services provided to participants.

39. The operator is obliged to manage undesired and unplanned events – incidents in order to provide a timely and effective response in the event information system security or functionality are jeopardised.

For the purposes of managing incidents within the meaning of paragraph 1 hereof, the operator shall establish procedures that shall in particular include detection, analysis, solving and recording such incidents.

40. With a view to safe and sound payment system operation, the operator is obliged to ensure that changes in the information system, including in particular changes in hardware and software, are tested and approved prior to being put into production, and to establish appropriate

procedures and the plan for restoring the system to the previous state in this regard.

For the purposes of managing the changes, the operator is obliged to ensure appropriate testing of such changes independently from the production environment.

Continuity of payment system operations

41. In case regular operation of a payment system is made impossible due to undesired and unexpected events, the operator shall ensure the continuity of the system's operations, taking into account requirements specified in this decision, as well as good business practices and generally accepted standards in the area.

42. In order to ensure the continuity of payment system operations, the operator should provide, based on the assessment of operational risk and analysis of its impact on operations, appropriate back-up solutions and adopt a business continuity plan for the payment system.

Back-up solutions shall pertain to resources, including in particular hardware, software, employees of the operator and services of persons to whom some operational activities relating to payment system operation have been outsourced.

The business continuity plan referred to in paragraph 1 of this Section shall represent one or more documents, including in particular:

1) description of procedures ensuring continuous operations of the payment system;
2) updated data on the resources referred to in paragraph 2 of this Section which are necessary for continuous operations of a payment system;
3) updated data on teams and members of teams responsible for plan implementation with clearly defined duties and responsibilities, as well as internal and external lines of communication.

The operator should specify the criteria for activation of the business continuity plan.

43. The operator shall, on a periodical basis and after the occurrence of significant changes, test the business continuity plan and ensure that participants and other persons relevant for payment system operation take part in regular or occasional testing.

The operator shall document the results of testing referred to in paragraph 1 of this Section and shall, taking into account potential confidentiality restrictions, communicate the results of such testing to the participants.

Managing other risks in the payment system

Minimum requirements regarding the outsourcing of operational activities of the operator to a third person

44. If the operator outsourced to a third person (hereinafter: service provider), pursuant to the Law, some operational activities relating to payment system operation – activities supporting the performance of activities in the payment system (hereinafter: operational activities), it shall also include the management of risks arising from such outsourcing in its risk management system.

45. Outsourcing of operational activities shall be based on a contract concluded between the operator and the service provider.

46. The operator shall oversee on an ongoing basis the performance of outsourced operational activities and their compliance with regulations, for the purpose of managing risks in the payment system.

Special requirements regarding management of risks in the payment system

47. The operator shall clearly define in payment system rules a daily schedule of the payment system and shall adhere to it consistently.

By way of derogation from paragraph 1 of this Section, the operator may depart from the daily schedule of the payment system only in cases specified in the system's rules, for the purpose of risk management.

If the operator allows the extension of payment system’s working hours at participants’ request, the payment system rules must clearly specify the conditions and manner of approval of such extension, and especially its duration.

48. If indirect participation in a payment system is allowed, the system's operator shall clearly define such participation in the payment system rules, as well as any appertaining rights and obligations.

Chapter 4

RISK MANAGEMENT IN IMPORTANT PAYMENT SYSTEMS

49. In order to adequately manage risks in an important payment system, in addition to the requirements specified in Chapter 3 of this Decision, its operator should also meet the requirements specified in this Chapter.

50. In order to adequately manage the financial risk, the operator of an important payment system should ensure liquid and low-risk collateral to cover its exposure and/or exposure of participants in the system to such risk, while applying value adjustment factors and restrictions regarding the concentration of such collateral.

51. In setting up the procedures referred to in Section 32 of this Decision, the operator of an important payment system may take into account key participants in such system, as well as their potential influence on other participants and the system as a whole.

The key participants referred to in paragraph 1 of this Section shall be identified in particular based on their participation in an important payment system, according to the number and value of transactions.

52. The operator of an important payment system should ensure that the back-up solutions and business continuity plan referred to in Section 42 of this Decision also include a back-up location at a distance from the primary location, taking into account the need to avoid the concurrent impact of the same risks on both locations.

The operator of an important payment system shall take all reasonable measures to ensure the continuation of key business processes relating to payment system operation not later than two hours after the occurrence of events that hinder regular operation of that system, and in any case to ensure the finalisation of settlement based on transfer orders by no later than the end of the day on which the settlement must take place.

The operator of an important payment system shall test the business continuity plan minimum once a year, in accordance with the requirements specified in Section 43 of this Decision.

Title III

REPORTING TO THE NATIONAL BANK OF SERBIA

53. An operator shall submit to the National Bank of Serbia data relating to payment system operation through regular and extraordinary reports.

54. The operator shall prepare the following regular reports:

1) Report on payment system operation – on RPS 1 – 4 forms (Attachment 1);
2) Report on conducted tests – on RIT form (Attachment 2);
3) Report on assessment of risk in the payment system;
4) Report on internal audit activities.

The content of forms referred to in paragraph 1, provisions 1) and 2) of this Section is specified in Attachments 1 and 2 enclosed with and integral to this Decision.

The report referred to in paragraph 1, provision 3) of this Section contains in particular information on threats, identified risks, assessment of risks and measures for addressing such risks with stipulated time limits for their application, information on implementation of measures for handling the risks specified in the previous report and the name, surname, phone number, email and signature of the person responsible for compiling and submitting such report.

The report referred to in paragraph 1, provision 4) of this Section shall contain in particular information on internal audit activities implemented in the previous year, internal audit plan for the current year and the name, surname, phone number, email and signature of the person responsible for compiling and submitting such report.

55. The operator shall submit the reports referred to in Section 54, paragraph 1, provision 1) of this Decision on a quarterly basis, no later than 15th calendar day in the month following the expiration of the reporting period.

The operator shall submit the reports referred to in Section 54, paragraph 1, provisions 2), 3) and 4) of this Decision on an annual basis, by no later than 31 March of the current year for the previous year.

56. The operator shall prepare the following extraordinary reports:

1) Report on materialisation of financial risk, and/or delay in payment system operation – on VIN form (Attachment 3);
2) Report on changes relating to payment system participants.

The content of the form referred to in paragraph 1, provision 1) of this Section is specified in Attachment 3 enclosed with and integral to this Decision.

The report referred to in paragraph 1, provision 2) of this Section should contain in particular the business name of the participant which underwent the change, the description of the change (the approach, including the manner of participation, exclusion, voluntary exit from the payment system, change in the manner of participation from indirect to direct etc.), the date when the change took place, the assessment of possible impact of the change on payment system operation, exposure of such system to risks, as well as the name, surname, phone number, email and signature of the person responsible for compiling and submission of the report.

57. The operator shall submit the reports referred to in Section 56 of this Decision within three business days from the day of materialisation of the financial risk, delay in payment system operation and/or occurrence of change in relation to participants in the system.

58. If the operator plans to implement changes in payment system operation, in particular changes relating to the information system, which may impact risk management in such system pursuant to this Decision, it shall submit to the National Bank of Serbia the action plan for implementation of such changes no later than 30 days before the start of their implementation.

The action plan referred to in paragraph 1 of this Section shall contain in particular the description of planned activities and their dynamics, the assessment of impact of changes in payment system operation on risk management in the system, as well as the name, surname, phone number, email and signature of the person responsible for compiling and submitting the report.

The obligations of the operator referred to in paragraph 1 of this Section are without prejudice to its obligation relating to amendments and supplements to payment system rules established in the Law.

59. The operator shall submit the reports specified in this part of the Decision in electronic form in accordance with the instruction of the National Bank of Serbia governing electronic data submission by the payment system operator.

Title V

CLOSING PROVISION

60. This Decision shall come into force on the eighth day following the day of its publication in the RS Official Gazette and shall apply as of 1 October 2015.

Decision No 4
2 June 2015
B e l g r a d e

G o v e r n o r
National Bank of Serbia

Dr Jorgovanka Tabaković