EXECUTIVE BOARD

OF THE NATIONAL BANK OF MOLDOVA

DECISION

No 12 of 11.01.2024

Approving the Regulation on strong customer authentication and open, common, and secure standard of communication between payment service providers

amended by Decision No 627 of 31.10.2024 of the Executive Board of the National Bank of Moldova, in force from 07.11.2024

Pursuant to Article 52^4 paragraph (7) of the Law No 114/2012 on Payment Services and Electronic Money (Official Monitor of the Republic of Moldova, 2012, No 193-197, Article 661), as amended, the Executive Board of the National Bank of Moldova.

DECIDES:

1. The Regulation on strong customer authentication and open, common, and secure standard of communication between payment service providers shall be approved (annexed).

2. This Decision shall enter into force on 1 February 2025, except for paragraph 72, which shall enter into force on the date of publication.
[Paragraph 2 amended by Decision No 627 of 31.10.2024 of the Executive Board of the National Bank of Moldova]

CHAIRMAN OF THE EXECUTIVE BOARD
No.12, Chisinau, 11.01.2024

Anca-Dana DRAGU

Approved by the
Decision of the Executive Board of the
National Bank of Moldova
No 12 of 11.01.2024

REGULATION
on strong customer authentication and open, common, and secure standard of communication between payment service providers

This Regulation transposes Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council on regulatory technical standards on strong customer authentication and open, common, and secure communication standards and Guideline EBA/GL/2018/07 on the conditions for an exemption from the emergency mechanism provided for in Article 33(6) of Regulation (EU) 2018/389.

CHAPTER I

GENERAL PROVISIONS

Section 1
SUBJECT MATTER

1. The Regulation lays down the requirements to be complied with by payment service providers in order to implement security measures enabling them the following:

1) to apply the strong customer authentication procedure in accordance with Article 52^4 of the Law on Payment Services and Electronic Money No 114/2012 (hereinafter - Law No 114/2012),

2) to be exempted from the application of the security requirements of strong customer authentication, subject to specific and limited conditions, depending on the level of risk, the amount and frequency of the payment transaction and the payment channel used for its execution,

3) to protect the confidentiality, integrity, and authenticity of the payment service user's personalised security credentials,

4) to implement the common and secure open standard of communication between account servicing payment service providers, payment initiation services providers, account information services providers, payers, payees and other payment service providers regarding the provision and use of payment services in accordance with Articles 52^1 - 52^4 of Law No 114/2012.

2. The terms and expressions used in this Regulation shall have the meaning of those laid down in Law No 114/2012 and in other regulatory acts issued by the National Bank of Moldova.

3. In addition, for the purposes of this Regulation, the following terms shall be used:

Information security skills - a set of specific knowledge evidenced by an expert certificate issued by a recognised entity enabling the auditor to make an opinion on the compliance of the payment service provider's security measures with the requirements laid down in this Regulation on the basis of information security knowledge.

Open, common, and secure standard of communication - a set of functional and technical specifications for the specific interfaces of payment service providers offering account management services, enabling payment initiation services providers, account information services providers and payment service providers issuing card-based payment instruments to access the payment accounts of payment service users.

Daily error response rate - the rate, calculated by the payment service provider offering online accessible payment account management services, of the number of error messages per day, which relate to errors attributable to the payment service provider offering online accessible payment account management services, sent by it to payment initiation services providers in a day, account information services providers and payment service providers issuing card-based payment instruments, in accordance with paragraphs 102 and 103, divided by the number of requests received on the same day by the payment service provider offering online accessible payment account management services from payment initiation services providers, account information services providers and payment service providers issuing card-based payment instruments.

Section 2
GENERAL AUTHENTICATION REQUIREMENTS

4. Payment service providers shall set up transaction monitoring mechanisms enabling them to identify unauthorised or fraudulent payment transactions in order to implement the security measures, prevention and limitation of unauthorised or fraudulent payment transactions,referred to in paragraph 1 subparagraphs 1) and 2).

These mechanisms shall be based on the analysis of payment transactions, considering specific features of the payment service user under normal use of personalised security credentials.

5. Payment service providers shall ensure that transaction monitoring arrangements are risk-based and consider, as a minimum, at least the following factors:

1) lists of compromised or stolen authentication elements,

2) amount of each payment transaction,

3) known fraud scenarios in relation to the provision of payment services,

4) indicators of compromised confidentiality, integrity, or authenticity of the session as a result of the authentication procedure,

5) record of normal and abnormal use of the access device or software provided to the payment service user by the payment service provider,

6) abnormal/unusual geographical location of the payer,

7) high-risk geographical location of the payee.

Section 3
REVIEW OF SECURITY MEASURES

6. The implementation of the security measures referred to in paragraph 1 shall be documented, tested, assessed, and audited at least every 3 years or at the request of the National Bank of Moldova by auditors with competence and experience in the field of information and payment security who are operationally independent of the payment service provider.

The period between the audits referred to in this paragraph shall be determined considering the relevant statutory accounting and audit framework applicable to the payment service provider.

7. Payment service providers making use of the derogation provided for in paragraphs 42 to 44 shall be audited at least once a year on the methodology for calculating fraud rates, the model used in calculating the fraud rate and the reported fraud rates, the process for calculating fraud rates being set out in paragraphs 45 to 47. The internal auditor carrying out this audit shall have expertise in information security and payments and shall be operationally independent of the payment service provider. During the first year in which the derogation set out in paragraphs 42 to 44 applies, and thereafter, at least every 3 years or more frequently, at the request of the National Bank of Moldova, this audit shall be carried out by an independent and qualified external auditor.

8. The audit referred to in paragraphs 6 and 7 shall be an assessment and report by the auditor on the compliance of the payment service provider's security measures with the requirements laid down in this Regulation. The report and the assessment shall be submitted to the National Bank of Moldova in accordance with the requirements laid down in Article 30 paragraph (3) of Law No 114/2012.

CHAPTER II
SECURITY MEASURES TO ENFORCE STRONG CUSTOMER AUTHENTICATION

Section 1
AUTHENTICATION CODE

9. In case payment service providers apply strong customer authentication in accordance with Article 52^4 paragraph (1) of Law No 114/2012, authentication shall be based on two or more features which are included in the category of knowledge, possession and inherence and result in the generation of an authentication code.

The authentication code is accepted only once by the payment service provider when the payer uses the authentication code to access his/her online payment account, to initiate an electronic payment transaction or to take any action through a remote channel that may involve a risk of payment fraud or other abuse.

10. For the purposes of paragraph 9, payment service providers shall adopt security measures ensuring that each of the following requirements is met:

1) no information on any of the elements referred to in paragraph 9 may be deduced from the disclosure of the authentication code,

2) no new authentication code can be generated based on knowledge of any other previously generated authentication code,

3) the authentication code cannot be falsified,

4) the code can only be used once,

5) the code is valid for a limited time.

11. Payment service providers shall ensure that authentication by means of an authentication code includes each of the following measures:

1) in case authentication for remote access, remote electronic payments and any other actions through a remote channel that may involve a risk of payment fraud or other abuse has failed to generate an authentication code within the meaning of paragraph 9, it shall not be possible to identify which of the features set out in paragraph 9 was incorrect,

2) the number of failed authentication attempts that may occur consecutively, after which the actions referred to in Article 52^4 paragraph (1) of Law No 114/2012 are temporarily or permanently blocked, shall not exceed five in a 15-minute period. In case the blocking is temporary, the duration of the blocking and the number of reattempts shall be determined on the basis of the characteristics of the service provided to the payer and all relevant risks involved, considering at least the factors set out in paragraph 5. Where the blocking has been made permanent, the payment service provider shall establish a secure procedure enabling the payer to regain access to electronic payment instruments. The payer shall be informed before the blocking becomes permanent,

3) communication sessions are protected against the capture of authentication data and manipulation by unauthorised parties, in accordance with the requirements set out in Chapter V,

4) communication session is invalidated if the payer does not perform any activity for five minutes after authentication.

Section 2
DYNAMIC LINKING

12. In case payment service providers apply strong customer authentication in accordance with Article 52^4 paragraph (2) of Law No 114/2012, in addition to the requirements set out in paragraphs 9 to 11 of this Regulation, they shall also adopt security measures that meet each of the following requirements:

1) the payer is informed of the amount of the payment transaction and of the payee,

2) the authentication code generated is specific to the amount of the payment transaction and the payee agreed by the payer at the time of initiating the payment transaction,

3) the authentication code accepted by the payment service provider corresponds to the initial specific amount of the payment transaction and to the identity of the payee agreed by the payer,

4) any change in the amount or payee invalidates of the generated authentication code.

13. For the purposes of paragraph 12, payment service providers shall adopt security measures to ensure, at all stages of the authentication process, the confidentiality, authenticity, and integrity of each of the following:

1) the amount of the payment transaction and the payee,

2) the information displayed to the payer, including the generation, transmission, and use of the authentication code.

14. For the purposes of paragraph 12 subparagraph 2) and in case payment service providers apply strong customer authentication in accordance with Article 52^4 paragraph (2) of Law No 114/2012, the following requirements for the authentication code shall apply:

1) in relation to a card-based payment transaction for which the payer has given consent to the exact amount of funds to be blocked pursuant to Article 60^1 paragraph (1) of Law No 114/2012, the authentication code shall be specific to the amount of funds to be

blocked for which the payer has given consent, and which was agreed by the payer at the time of the initiation of the transaction,

2) in relation to payment transactions for which the payer has given consent to the execution of a batch (bundle of instructions) of remote electronic payment transactions to one or more payees, the authentication code shall be specific to the total amount of the batch of payment transactions and to the specified payees.

Section 3
STRONG AUTHENTICATION ELEMENT REQUIREMENTS

15. Payment service providers shall adopt security measures to mitigate the risk that elements of:

a) strong customer authentication classified as knowledge being read by or disclosed to unauthorised parties. The payer's use of these elements shall be subject to mitigation measures to prevent their disclosure to unauthorised parties,

b) strong authentication of customers classified as possessions to be used by unauthorised parties. The payer's use of such elements shall be subject to measures designed to prevent replication of the elements,

c) authentication that is classified as inherent and read by access devices and software provided to the payer is read by unauthorised parties. As a minimum condition, payment service providers shall ensure that the access devices and software in question have a very low probability that an unauthorised party is authenticated as the payer. The payer's use of such elements shall be subject to measures to ensure that such devices and software resist unauthorised use of the features through access to those devices and software.

16. Payment service providers shall ensure that the use of the elements of strong customer authentication referred to in paragraph 15, in terms of their technology, algorithms and parameters, are subject to measures to ensure that the breach of one element does not compromise the reliability of the other elements.

17. Payment service providers shall implement security measures, where any of the elements of strong customer authentication or the authentication code itself are used through a universal device, to mitigate the risk that would result from the compromise of that universal device. Mitigation measures include each of the following:

1) use of secure execution environments, separated by software installed on the universal device,

2) mechanisms to ensure that the software or device has not been modified by the payer or a third party,

3) where changes have occurred to the systems managing elements of strong authentication and authentication codes on the universal device, mechanisms to mitigate their consequences.

CHAPTER III
DEROGATIONS FROM STRONG CUSTOMER AUTHENTICATION

Section 1
ACCESS TO PAYMENT ACCOUNT INFORMATION DIRECTLY FROM THE PAYMENT SERVICE PROVIDER OFFERING ACCOUNT MANAGEMENT SERVICES

18. Payment service providers shall be allowed not to apply strong customer authentication, subject to compliance with the requirements laid down in paragraphs 4 and 5, where a payment service user accesses payment account online, directly, provided that access is limited to one of the following online elements, without disclosure of sensitive payment data:

1) balance of one or more payment accounts designated by the user,

2) payment transactions executed within the last 90 days through one or more payment accounts designated by the user.

19. For the purposes of paragraph 18, payment service providers shall not be exempted from the application of strong customer authentication if any of the following conditions are met:

1) payment service user accesses online the information specified in paragraph 18 for the first time,

2) more than 180 days have elapsed since the payment service user last accessed online the information specified in paragraph 18 and strong customer authentication was applied.

Section 2
ACCESS TO PAYMENT ACCOUNT INFORMATION THROUGH AN ACCOUNT INFORMATION SERVICE PROVIDER

20. Payment service providers shall not apply strong customer authentication where a payment service user accesses payment account online through an account information service provider, as long as access is limited to one of the following online elements, without disclosure of sensitive payment data:

1) balance of one or more designated payment accounts,

2) payment transactions executed within the last 90 days through one or more designated payment accounts.

21. By way of derogation from paragraph 20, payment service providers shall apply strong customer authentication if one of the following conditions is met:

1) payment service user accesses the information specified in paragraph 20 online for the first time through the account information service provider,

2) more than 180 days have elapsed since the payment service user last accessed online the information referred to in paragraph 20 through the account information service provider and strong customer authentication was applied.

22. By way of derogation from paragraph 20, payment service providers shall apply strong customer authentication where a payment service user accesses payment account online through an account information service provider and the payment service provider has justified reasons, supported by appropriate evidence, relating to unauthorised or fraudulent access to the payment account. In such a case, the payment service provider shall, upon request, duly document and justify to the National Bank of Moldova the reasons for applying strong customer authentication.

23. Payment service providers offering account management services which provide a specific interface as referred to in paragraph 75, shall not be obliged to implement the derogation provided for in paragraph 20 in the context of the implementation of the emergency mechanism provided for in paragraph 86, if they do not apply the derogation provided for in paragraphs 18 and 19 in the direct interface used for authentication and communication with their payment service users.

Section 3
CONTACTLESS PAYMENTS MADE AT POINT OF SALE

24. Payment service providers shall have the right not to apply strong customer authentication, subject to compliance with the requirements set out in paragraphs 4 and 5, where the payer initiates an electronic contactless payment transaction by means of a payment instrument with contactless functionality where the individual value of the electronic contactless payment transaction does not exceed MDL 1,000 or the foreign currency equivalent if one of the following conditions is met:

1) cumulative value of contactless electronic payment transactions initiated by a payer since the date of the last application of strong customer authentication does not exceed MDL 3,000 or the foreign currency equivalent,

2) number of consecutive contactless electronic payment transactions initiated since the date of the last application of strong customer authentication does not exceed five.

Section 4

UNATTENDED TERMINALS FOR TRANSPORT TICKETS AND PARKING FEES

25. Payment service providers shall have the right not to apply strong customer authentication, subject to compliance with the requirements set out in paragraphs 4 and 5 in case the payer initiates an electronic payment transaction at an unattended payment terminal (unattended ATMs) in order to pay for a transport ticket or a parking fee.

Section 5
TRUSTED BENEFICIARIES

26. Payment service providers shall apply strong customer authentication when a payer creates or amends a list of trusted beneficiaries through the payment service provider managing the payer's account.

27. Payment service providers shall have the right not to apply strong customer authentication, subject to compliance with the requirements set out in paragraphs 4 and 5, in case the payer initiates a payment transaction, and the payee is on a list of trusted beneficiaries previously created by the payer.

Section 6
RECURRING TRANSACTIONS

28. Payment service providers shall apply strong customer authentication when a payer creates, changes or initiates for the first time a series of recurring transactions of the same value with the same payee.

29. Payment service providers shall have the right not to apply strong customer authentication, subject to compliance with the requirements set out in paragraphs 4 and 5, for the initiation of all subsequent payment transactions included in the series of payment transactions set out in paragraph 28.

Section 7
CREDIT TRANSFERS BETWEEN ACCOUNTS HELD BY THE SAME NATURAL OR LEGAL PERSON

30. Payment service providers shall have the right not to apply strong customer authentication, subject to compliance with the requirements set out in paragraphs 4 and 5 in case a credit transfer transaction is initiated where the payer and the payee are one and the same natural or legal person and both payment accounts are held by the same payment service provider managing the account.

Section 8
LOW-VALUE TRANSACTIONS

31. Payment service providers shall have the right not to apply strong customer authentication, subject to compliance with the requirements set out in paragraphs 4 and 5, in case the payer initiates a remote electronic payment transaction for a value not exceeding MDL 600 or the foreign currency equivalent which meets one of the following conditions:

1) the cumulative value of previous remote electronic payment transactions initiated by a payer since the last application of strong authentication does not exceed MDL 2,000 or the foreign currency equivalent,

2) the number of previous remote electronic payment transactions initiated by the payer since the last application of strong customer authentication does not exceed 5 such consecutive individual transactions.

Section 9
SECURE PAYMENT PROCESSES AND PROTOCOLS.

APPROVAL OF STRONG CUSTOMER AUTHENTICATION EXEMPTION

32. Payment service providers shall have the right not to apply strong customer authentication, subject to compliance with the requirements set out in paragraphs 4 and 5, to legal entities initiating electronic payment transactions using specific payment processes or protocols that are made available only to non-consumer payers, if the National Bank of Moldova considers that these processes or protocols guarantee security levels at least equivalent to those set out in Law No 114/2012. In order to benefit from the exception from the obligation to apply strong customer authentication, payment service providers that provide customers with specific payment processes or protocols used exclusively by non-consumers shall apply to the National Bank of Moldova for the granting of this exception.

33. In order to grant an exemption from the obligation to apply strong customer authentication referred to in paragraph 32, the National Bank of Moldova shall consider compliance with the following requirements:

1) payment service provider has a system for monitoring payment transactions initiated through specific payment processes or protocols which are made available only to non-consumer payers,

2) payment service provider has a secure communication system that complies with the requirements of this Regulation (including aspects of data encryption, confidentiality, and integrity of customised security credentials),

3) payment service provider uses a secure method of customer authentication to ensure that the risk of authentication by an unauthorised person is mitigated.

34. In assessing and monitoring the compliance of payment service providers with the requirements of paragraphs 32 and 33, the National Bank of Moldova shall consider the fraud rates recorded by the payment service providers concerned. The fraud rate shall be calculated as the cumulative value of remote payment transactions considered to be fraudulent, for which strong customer authentication has been applied, and payment transactions carried out using specific payment processes or protocols that are made available to non-consumer payers, multiplied by the total value of remote payment transactions, regardless of whether strong customer authentication has been applied or executed using specific payment processes or protocols that are made available to non-consumer payers.

All fraudulent payment transactions shall be included, regardless of whether the funds have been recovered or not. The calculation shall be made on a quarterly basis and the reference rate used for currency conversions shall be the average reference rate of the National Bank of Moldova for the quarter for which the fraud rates are calculated.

35. The payment service provider intending to obtain exemption from the obligation to apply strong customer authentication shall submit to the National Bank of Moldova an application for granting the exemption, annexing the following documents and information:

1) a detailed audit report that shall record the compliance of specific payment processes and protocols with the requirements laid down in Articles 32^1 and 32^2 of Law No 114/2012 and paragraphs 4-8, 53-61, 95-100 of this Regulation and other normative acts of the National Bank of Moldova in the field of security measures concerning operational and security risks related to payment services. In addition, the applicant payment service provider shall submit to the National Bank of Moldova the affidavit of the person who audited the specific payment processes or protocols (as part of the payment service provider's IT system or independently) regarding its operational independence from the payment service provider and the IT security certifications held, as well as payment expertise,

2) the level of fraud rate for payment transactions initiated through specific payment processes and protocols. These shall be reported to the National Bank of Moldova on a quarterly basis.

36. The application for exemption from the obligation of strong customer authentication, documents and information annexed thereto shall be submitted to the

National Bank of Moldova in Romanian language in original or certified copies. If the documents and information are drawn up in a foreign language, they shall be submitted in original or certified copies, with the certified translation into Romanian language annexed.

37. The application and the documents referred to in paragraph 35 shall be submitted to the National Bank of Moldova by the governing body/member thereof or the person empowered by legislation (showing that the person is authorised to represent the applicant in relation to the National Bank of Moldova).

38. Within 30 days from the date of receipt of the complete set of documents in accordance with paragraph 35, the National Bank of Moldova shall decide whether to grant an exemption from the obligation to apply strong customer authentication or to reject the application, informing the payment service provider of its decision. The National Bank of Moldova may set, by informing the payment service provider, a longer term for issuing the decision, which shall not exceed 90 days, under the conditions of the Administrative Code of the Republic of Moldova.

39. If the set of documents submitted to the National Bank of Moldova is not complete and the payment service provider does not submit within the deadline established by the National Bank of Moldova the documents necessary for its completion, the National Bank of Moldova shall inform the payment service provider about the termination of the administrative procedure, upon expiry of 3 working days from the deadline set by the National Bank of Moldova.

40. If the documents or information submitted in accordance with paragraph 35 are insufficient for the decision to be taken, the National Bank of Moldova may request additional documents and information. The payment service provider shall submit additional information and documents within the time limit specified by the National Bank of Moldova, during which period the time limit set by the National Bank of Moldova in accordance with paragraph 38 shall be suspended.

41. The National Bank shall reject the application for exemption from the obligation to apply strong customer authentication if:

a) following the assessment of all documents and information held, the National Bank of Moldova finds that the requirements set out in paragraphs 32 and 33 are not met; and/or

b) the submission to the National Bank of Moldova of erroneous, inauthentic and/or contradictory information and documents.

Section 10
RISK ANALYSIS OF TRANSACTIONS

42. Payment service providers shall have the right not to apply strong customer authentication in case the payer initiates a remote electronic payment transaction identified by the payment service provider as low risk in accordance with the transaction monitoring mechanisms set out in paragraphs 4-5 and paragraph 43 subparagraph 3).

43. Electronic payment transactions shall be considered to present a low level of risk if the following conditions are cumulatively met:

1) fraud rate for this type of transaction, reported by the payment service provider and calculated in accordance with paragraphs 45-47, shall be equal to or lower than the reference fraud rate specified in the table provided in Annex No 1,
2) value of the transaction does not exceed the relevant derogation threshold value set out in the table provided in Annex No 1,
3) payment service providers have not identified any of the following features, following a real-time risk analysis through transaction monitoring mechanisms:

a) abnormal expenditure or an abnormal pattern of payer behaviour,
b) unusual information about the payer's access to the device/software,
c) malware infection in any session of the authentication process,
d) known fraud scenarios in relation to the provision of payment services.

44. The assessment carried out by a payment service provider shall combine all risk-based factors referred to in paragraph 43 subparagraph 3) into a single risk scoring system for each individual transaction in order to determine whether a particular payment should be allowed without strong customer authentication.

Section 11
CALCULATION OF FRAUD RATES

45. For each type of transaction listed in the table provided in Annex No 1, the payment service provider shall ensure that the overall fraud rates for all types of payment transactions are equivalent to or do not exceed the reference fraud rates for the same type of payment transaction listed in the table provided in Annex No 1.

46. The overall fraud rate for each type of transaction shall be calculated quarterly as the total value of unauthorised or fraudulent remote transactions, whether or not funds have been recovered, divided by the total value of all remote transactions of the same type.

47. The methodology and models used by the payment service provider to calculate fraud rates, as well as the fraud rates themselves, shall be duly documented and submitted in full to the National Bank of Moldova upon its request.

Section 12
CESSATION OF DEROGATIONS BASED ON RISK ANALYSIS OF TRANSACTIONS

48. Payment service providers that make use of the derogation provided for in paragraphs 42-44 shall immediately inform the National Bank of Moldova if any of their monitored fraud rates for any type of payment transaction listed in the table provided in Annex No 1 is higher than the applicable fraud reference rate and shall provide the National Bank of Moldova with a description of the measures they intend to take to restore the compliance of their monitored fraud rates with the applicable reference fraud rates.

49. Payment service providers shall immediately cease to use the derogation provided for in paragraphs 42 to 44 for any type of payment transaction listed in the table provided in Annex No 1 and falling within the specific derogation threshold range, if the fraud rate monitored by them exceeds for two consecutive quarters the reference fraud rate applicable for that payment instrument or type of payment transaction in that derogation threshold range.

Following the cessation of the derogation provided for in paragraphs 42 to 44, payment service providers shall no longer use that derogation until the fraud rate calculated for a quarter is equal to or lower than the reference fraud rates applicable for that type of payment transaction in that derogation threshold range.

50. In case payment service providers intend to make use again of the derogation provided for in paragraphs 42 to 44, they shall inform the National Bank of Moldova and provide evidence, before making use again of the derogation, of the restoration of compliance of the fraud rate monitored by them with the reference fraud rates applicable for the respective derogation threshold range.

Section 13
MONITORING

51. In order to make use of the derogations from the application of strong customer authentication, payment service providers shall record and monitor the data below for each type of payment transaction, with a separation for both remote and non-remote payment transactions, at least once a quarter:

1) the total amount of unauthorised payment transactions, including fraudulent ones in accordance with Article 52 paragraph (2) of Law No 114/2012, the total amount of all payment transactions and the related fraud rate, including a breakdown of payment transactions initiated through strong customer authentication and those made under each derogation,

2) the average transaction value, including a breakdown of payment transactions initiated through strong customer authentication and those initiated under each derogation,

3) the number of payment transactions for which each of the derogations has been applied and their proportion in relation to the total number of payment transactions.

52. Payment service providers shall submit the results of the monitoring carried out in accordance with paragraph 51 to the National Bank of Moldova upon its request.

CHAPTER IV
CONFIDENTIALITY AND INTEGRITY OF PERSONALISED SECURITY CREDENTIALS OF PAYMENT SERVICE USERS

53. Payment service providers shall ensure the confidentiality and integrity of personalised security credentials of payment service users, including authentication codes, during all phases of authentication by implementing at least the following requirements:

1) personalised security credentials are masked as they are entered by the payment service user during authentication,

2) personalised security credentials in data format and cryptographic material related to the encryption of personalised security credentials shall not be stored in plain text,

3) secret cryptographic material is protected against unauthorised disclosure,

4) personalised security credentials are created in a secure environment. They implement measures to mitigate the risks of unauthorised use of personalised security credentials, devices, or software used for authentication,

5) processing and transmission of personalised security credentials and authentication codes generated in accordance with Chapter II shall take place in secure environments in accordance with professional standards in the field and which are widely recognised,

6) transmission of personalised security credentials and authentication devices and software to the payment service user is carried out in a secure manner designed to counter the risks of unauthorised use due to loss, theft or copying. For this purpose, payment service providers shall implement, as a minimum requirement, each of the following measures:

a) effective and secure transmission mechanisms ensuring that personalised security credentials and authentication software and devices are transmitted to the legitimate payment service user,

b) mechanisms allowing the payment service provider to verify the authenticity of the authentication software transmitted to the payment services user via the Internet,

c) arrangements to ensure that where the transmission of personalised security credentials is executed off-premises or through a remote channel, the payment service provider shall ensure that the personalised security credentials are transmitted to the payment service user:

– No unauthorised party may obtain more than one component of the personalised security credentials or authentication devices or software when transmitted through the same channel,

– personalised security credentials or authentication software or devices transmitted shall be activated before use,

d) arrangements to ensure that in case personalised security credentials or authentication devices or software need to be activated before first use, activation takes place in a secure environment in accordance with the pairing procedures set out in paragraph 55.

54. Payment service providers shall fully document the process related to the management of cryptographic materials used to encrypt or render unreadable personalised security credentials.

55. Payment service providers shall ensure that only the payment service user is securely associated with personalised security credentials, authentication devices and software. For that purpose, payment service providers shall ensure that each of the following requirements is met:

1) association of the payment service user's identity with the personalised security credentials and authentication devices and software shall be carried out in secure environments under the responsibility of the payment service provider; in this context, at least the premises of the payment service provider, the Internet environment provided by the payment service provider or other similar secure websites used by the payment service provider, and the payment service provider's ATM services shall be considered. The risks associated with devices and their components which are used during the association process, and which are not under the responsibility of the payment service provider shall also be considered,

2) association through a remote channel of the identity of the payment service user with personalised security credentials and authentication devices or software shall be carried out by means of strong customer authentication.

56. Payment service providers shall ensure that the renewal or reactivation of personalised security credentials follows the procedures for the creation, association and transmission of security credentials and authentication devices in accordance with paragraphs 53 to 55.

57. Payment service providers shall ensure that they have effective procedures in place to implement each of the following security measures:

1) secure destruction, deactivation or revocation of personalised security credentials and authentication devices and software,

2) in case payment service provider distributes reusable authentication devices and software, the secure reuse of a device or software shall be established, documented, and implemented before it is made available to another payment service user,

3) disabling or revoking information related to personalised security credentials stored in the payment service provider's systems and databases and, where relevant, in public registers.

CHAPTER V
OPEN, COMMON AND SECURE STANDARD OF COMMUNICATION

Section 1
GENERAL COMMUNICATION REQUIREMENTS

58. Payment service providers shall ensure that secure identification conditions are in place for communication between the payer's device and the payee's devices accepting electronic payments, including but not limited to payment terminals.

59. Payment service providers shall ensure that the risks of misdirection of communication to unauthorised persons in mobile applications and other interfaces of payment service users offering electronic payment services are effectively mitigated.

60. Payment service providers shall establish procedures to ensure that all payment transactions and other interactions, carried out in the context of the provision of payment services, with the payment service user, other payment service providers and other entities, including merchants, can be traced, ensuring that ex post information is available on all events relevant to the electronic transaction at any stage.

61. For the purposes of paragraph 60, payment service providers shall ensure that any communication session with the payment service user, other payment service providers and other entities, including merchants, is based on each of the following features:

1) a unique identifier of the session,

2) security mechanisms for the detailed recording of the transaction, including transaction number, timestamps, and all relevant transaction data,

3) time stamps that are based on a unique time reference system and that are synchronised according to an official time signal.

Section 2
SPECIFIC REQUIREMENTS FOR AN OPEN, COMMON AND SECURE STANDARD OF COMMUNICATION

Section 1
GENERAL OBLIGATIONS FOR ACCESS INTERFACES

62. Payment service providers that offer account management services and provide a payer with an online accessible payment account shall have, as a minimum, an interface that meets each of the following requirements:

1) account information services providers, payment initiation service providers and payment service providers issuing card-based payment instruments shall be able to identify themselves to the payment service provider offering account management services,

2) account information services providers shall be able to communicate securely in order to request and receive information on one or more payment accounts designated by the user and the related payment transactions,

3) payment initiation services providers shall be able to communicate securely in order to initiate a payment order from the payer's payment account and to receive all information relating to the initiation of the payment transaction and all information to which payment service providers offering account management services have access in relation to the execution of the payment transaction.

63. For the purposes of payment service user authentication, the interface provided for in paragraph 62 shall allow account information service providers and payment initiation service providers to rely on all authentication procedures provided by the payment service provider offering account management services to the payment service user.

64. The interface shall at least meet the following requirements:

1) a payment initiation service provider or an account information service provider shall be able to require the payment service provider offering account management services to begin authentication on the basis of the payment service user's consent given to the payment initiation service provider or account information service provider,

2) communication sessions between the payment service provider offering account management services, the account information service provider, the payment initiation service provider, and any payment service user concerned shall be established and maintained for the duration of the authentication,

3) integrity and confidentiality of personalised security features and authentication codes transmitted by or through the payment initiation service provider or account information service provider shall be guaranteed by all payment service providers.

65. Payment service providers offering account management services shall ensure that their interfaces comply with the open, common, and secure standard of communication issued by international or European standardisation organisations as set out in the functional and technical requirements issued by the National Bank of Moldova.

66. Payment service providers offering account management services shall also ensure that the technical specifications of any interface developed under the open, common and secure standard of communication are documented with information specifying the routine processes, protocols and tools required by payment initiation service providers, account information service providers and payment service providers issuing card-based payment instruments to enable their software and applications to be interoperable with the systems of payment service providers offering account management services.

67. Payment service providers offering account management services shall make the documentation available, free of charge, at the request of licensed payment initiation service providers, licensed account information service providers and licensed payment service providers issuing card-based payment instruments or payment service providers that have applied to the National Bank of Moldova for the relevant licence and shall make the summary of the documentation publicly available on their website.

68. In addition to the requirements set out in paragraphs 65 to 67, payment service providers offering account management services shall ensure that, except in emergency situations, any changes to the technical specifications of their interface are made available to licensed payment initiation service providers, licensed account information service providers and licensed payment service providers issuing card-based payment instruments or payment service providers that have applied to the National Bank of Moldova for the relevant licence, in advance, as soon as possible and at least 3 months before the implementation of the change.

69. Payment service providers shall document emergency situations in which changes have been made and submit the documentation to the National Bank of Moldova upon request.

70. By way of derogation from paragraphs 68 and 69, payment service providers offering account management services shall submit to payment service providers amendments to the technical specifications of their interfaces to comply with paragraphs 20 to 23 at least 2 months before the implementation of these amendments.

71. Payment service providers offering account management services shall provide a test platform, including related support, for connection and functional testing, to enable licensed payment initiation service providers, licensed account information service providers and licensed payment service providers issuing card-based payment instruments or payment service providers that have applied to the National Bank of Moldova for the relevant licence to test the software and applications used to provide a payment service to users.

72. The test platform referred to in paragraph 71 shall be made available no later than three months before the planned market launch of the access interface. However, no sensitive information shall be made available through the test platform.

73. The National Bank of Moldova shall ensure that payment service providers offering account management services comply at all times with the obligations included in the open, common, and secure standard of communication with regard to the interface(s) they have established.

74. In case a payment service provider offering account management services does not comply with the requirements for interfaces set out in the communication standard, the National Bank of Moldova shall ensure that the provision of payment initiation services and account information services is not hindered or disrupted, provided that such payment service providers comply with the conditions set out in paragraphs 87 and 88.

Subsection 2
ACCESS INTERFACE OPTIONS

75. Payment service providers offering account management services shall establish the interface(s) provided for in paragraphs 62 to 74 by means of a specific interface or grant the payment service providers referred to in paragraph 62 the right to use the interfaces used for authentication and communication with the payment service users of the payment service provider offering account management services.

Subsection 3
SPECIFIC INTERFACE OBLIGATIONS

76. Subject to paragraphs 62-75, payment service providers offering account management services which have established a specific interface shall ensure that the specific interface offers at all times the same level of availability and performance,

including support, as the interfaces made available to the payment service user for direct access to the online payment account.

77. Payment service providers offering account management services that have established a specific interface shall define key performance indicators and transparent service level targets that are at least as stringent as those set for the interface used by their payment service users, both in terms of availability and data provided in accordance with paragraphs 101-106. These interfaces, indicators and targets shall be monitored by the National Bank of Moldova and stress-tested by payment service providers offering account management services.

78. Payment service providers offering account management services that have established a specific interface shall ensure that this interface does not create obstacles to the provision of payment initiation and account information services.

79. The obstacles referred to in paragraph 78 include, inter alia, preventing the use by payment service providers referred to in paragraph 62 of security elements issued by payment service providers offering account management services to their customers, requiring redirection to the authentication service of the payment service provider offering account management services or to other functions of that payment service provider, requiring additional authorisations and registrations in addition to those provided for in Section 1 of Chapter III of Law No 114/2012 or requiring additional checking on the consent given by payment service users to payment initiation service providers and account information service providers.

80. For the purposes of paragraphs 76 and 77, payment service providers offering account management services shall monitor the availability and performance of the specific interface.

81. Payment service providers offering account management services shall publish on their website quarterly statistics on the availability and performance of the specific interface and the interface used by their payment service users.

Subsection 4
EMERGENCY MECHANISM FOR THE SPECIFIC INTERFACE

82. Payment service providers offering account management services shall, when designing the specific interface, provide for the emergency mechanism strategy and plans for situations where the specific interface does not function in accordance with paragraphs 76-81 or experiences unforeseen downtime or where the system ceases to function.

83. An unplanned downtime or system shutdown may be deemed to have occurred when five consecutive requests for access to information for the provision of payment initiation or account information services are not responded to within 30 seconds.

84. Emergency measures shall include communication plans to provide payment service providers using the specific interface with information on system recovery measures and a description of immediately available alternative options that payment service providers have in the meantime.

85. Both the payment service provider offering account management services and the payment service providers referred to in paragraph 62 shall report to the National Bank of Moldova without delay on problems related to the specific interfaces described in paragraphs 82, 83.

86. As part of an emergency mechanism, payment service providers referred to in paragraph 62 shall have the right to use, until the specific interface returns to the level of availability and performance set out in paragraphs 76 to 81, the interfaces made available to payment service users for authentication and communication with their payment service provider offering account management services.

87. For this purpose, payment service providers offering account management services shall ensure that the payment service providers referred to in paragraph 62 can be identified and can rely on the authentication procedures provided by the payment service provider offering account management services to payment service users.

88. In case of using the interface provided for in paragraph 86, the payment service providers referred to in paragraph 62 shall:

1) take the necessary steps to ensure that they do not access, store, or process data for purposes other than the provision of the service requested by the payment service user,

2) continue to comply with the obligations arising from Articles 52^2 paragraph (3) and 52^3 paragraph (2) of Law No 114/2012,

3) record data that are accessed through the interface operated by the payment service provider offering account management services to its payment service users and provide the recorded data to the National Bank of Moldova upon request and without undue delay,

4) duly justify to the National Bank of Moldova, upon request and without undue delay, the use of the interface provided to payment service users for the purpose of direct access to their online payment account,

5) inform the payment service provider offering account management services to this effect.

89. Payment service providers offering account management services that have opted for a specific interface shall be exempted, in accordance with Chapter VI, by the National Bank of Moldova from the obligation to set up the emergency mechanism described in paragraph 86 if the specific interface meets all of the following conditions:

1) it complies with all the obligations relating to specific interfaces set out in paragraphs 76 to 81,

2) it has been designed and tested in accordance with paragraphs 71 and 72 in a way that is satisfactory to the payment service provider referred to in that Article,

3) it has been widely used for at least three months by payment service providers to provide account information and payment initiation services and to confirm the availability of funds for card payments,

4) any problems with the specific interface have been resolved without undue delay.

90. The National Bank of Moldova shall withdraw the exemption provided for in paragraph 89 if the conditions in paragraph 89 subparagraphs 1) and 4) are not met by payment service providers offering account management services for more than two consecutive calendar weeks. The National Bank of Moldova shall inform the payment service provider offering account management services of the revocation. In doing so, the National Bank of Moldova shall ensure that the payment service provider offering account management services establishes, as soon as possible and within two months at most, the emergency mechanism referred to in paragraph 86.

Subsection 5
CERTIFICATES

91. For the purposes of identification as referred to in paragraph 62 subparagraph 1), payment service providers shall rely on qualified certificates for electronic seals or website authentication as defined in the Law on Electronic Identification and Trust Services No 124/2022.

92. For the purposes of this Regulation, the registration number referred to in the official registers, which is provided for in the Law on Electronic Identification and Trust Services No 124/2022, is the authorisation number of payment service providers issuing card-based payment instruments, account information service providers and payment initiation service providers, including payment service providers offering account management services and providing such services, number that is available in the public register pursuant to Article 23 of Law No 114/2012 or resulting from the authorisations granted pursuant to the Law on the Activity of Banks No 202 /2017.

93. For the purposes of this Regulation, qualified certificates for electronic seals or for website authentication referred to in paragraph 91 shall include, in a language customarily used in the sphere of international finance, additional specific attributes in relation to each of the following:

1) the role of the payment service provider, which may be one or more of the following:

a) provision of account management services,

b) provision of payment initiation services,

c) provision of account information services,

d) issuance of card-based payment instruments,

2) name of the competent authorities with which the payment service provider is registered, i.e., the National Bank of Moldova.

94. The attributes set out in paragraph 93 shall not affect the interoperability and recognition of qualified certificates for electronic seals or for website authentication.

Subsection 6

SECURITY OF COMMUNICATION SESSIONS

95. Payment service providers offering account management services, payment service providers issuing card-based payment instruments, account information service providers and payment initiation service providers shall ensure that, when data is exchanged over the Internet, secure encryption processes are applied between communicating parties throughout the communication session to protect the confidentiality and integrity of data, using robust and widely recognised encryption techniques.

96. Payment service providers issuing card-based payment instruments, account information service providers and payment initiation service providers shall keep the duration of the access sessions offered by payment service providers offering account management services as short as possible and actively terminate such sessions as soon as the requested action has been completed.

97. When maintaining parallel network sessions with the payment service provider offering account management services, account information service providers and payment initiation service providers shall ensure that those sessions are securely linked to the relevant sessions established with the payment service user(s), in order to avoid the risk that any message or information communicated between them is transmitted to the wrong destination.

98. Account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments together with the payment service provider offering account management services shall indicate explicit references to each of the following:

1) payment service user(s) and the corresponding communication sessions, in order to distinguish between multiple requests from the same payment service user(s),

2) for payment initiation services, the uniquely identified initiated payment transaction,

3) for confirmation of the availability of funds, the uniquely identified request for the amount required to execute the card payment transaction.

99. Payment service providers offering account management services, account information service providers, payment initiation service providers and payment service providers issuing card payment instruments shall ensure that in case they communicate personalised security credentials and authentication codes, these cannot be read, directly or indirectly, by any member of staff at any time.

100. In the event of loss of confidentiality of personalised security credentials when they are within the scope of their competence, the providers concerned shall inform without delay the user of the related payment services and the issuer of the personalised security features thereof.

101. Payment service providers offering account management services shall comply with each of the following requirements:

1) they shall provide account information service providers with the same information from the user's designated payment accounts and related payment

transactions as is made available to the payment service user when the latter requests direct access to account information, provided that such information does not include sensitive payment data,

2) they shall provide payment initiation service providers, immediately upon receipt of the payment order, with the same information on the initiation and execution of the payment transaction as that provided or made available to the payment service user where the payment transaction is initiated directly by the payment service user,

3) they shall, on request, immediately inform payment service providers, by means of a confirmation in a simple “yes” or “no” format, whether the amount needed to execute a payment transaction is available on the payer's payment account.

102. In case of an unexpected event or error occurring during the identification or authentication process or during the exchange of information, the payment service provider offering account management services shall send a notification message to the payment initiation service provider or account information service provider and the payment service provider issuing card payment instruments explaining why the unexpected event or error occurred.

103. In case the payment service provider offering account management services provides a specific interface in accordance with paragraphs 76 to 81, the interface shall make available notification messages relating to unexpected events or errors to be communicated by any payment service provider detecting the event or error to the other payment service providers participating in the communication session.

104. Account information service providers shall have adequate and effective mechanisms in place to prevent access to information other than that from the user's designated payment accounts and related payment transactions, in accordance with the user's explicit consent.

105. Payment initiation service providers shall provide payment service providers offering account management services with the same information as that required by the payment service user when initiating the payment transaction directly.

106. Account information service providers shall be able to access information from the payment accounts designated by the user and the related payment transactions held by payment service providers offering account management services for the execution of the account information service in any of the following circumstances:

1) whenever the payment service user actively requests such information,

2) in case the payment service user does not actively request such information, no more than four times within a 24-hour period, unless the account information service provider and the payment service provider offering account management services have agreed on a higher frequency with the consent of the payment service user.

CHAPTER VI
APPROVAL OF THE EXEMPTION FROM THE OBLIGATION TO ESTABLISH THE EMERGENCY MECHANISM PROVIDED FOR IN ITEM 82

107. This Chapter shall apply to payment service providers that offer payment account management services accessible online and provide specific interfaces that allow third party payment service providers to access payment accounts.

108. This Chapter lays down the requirements to be met by payment service providers offering online accessible payment account management services in order to benefit from the exemption from the obligation to set up the emergency mechanism, as provided for in paragraph 89.

109. In order to grant exemption from the obligation to establish the emergency mechanism referred to in paragraph 82, the National Bank of Moldova shall assess whether the payment service provider fulfils the conditions set out in paragraph 89, the requirements set out in Attachment 3 of this Regulation and the provisions of Law No 114/2012.

110. A payment service provider intending to obtain an exemption from the obligation to establish the emergency mechanism referred to in paragraph 82 shall submit to the National Bank of Moldova an application for granting the exemption, in accordance with Attachment 2 of this Regulation, with the following documents and information annexed:

1) information and documents proving compliance with the requirements set out in Attachment 3 and proof of approval of the application by the governing body or senior management of the payment service provider, as appropriate,

2) information and documents proving compliance with the conditions set out in paragraph 89 of this Regulation.

111. The payment service provider shall submit a request, in accordance with paragraph 110 for each specific interface provided for which it is intended to be exempted from the obligation to set up the emergency mechanism.

112. If a payment service provider considers that one of the requirements set out in Attachment 3 does not apply to it, it shall state in the documentation submitted to the National Bank of Moldova the reason why that requirement does not apply to it.

113. Applications for exemption from the obligation to establish the emergency mechanism referred to in paragraph 82, the documents and information attached thereto shall be submitted to the National Bank of Moldova in Romanian language in original or certified copies. If the documents and information are drawn up in a foreign language, they shall be submitted in the original or certified copies, with the certified translation into the Romanian language annexed.

114. The documents referred to in paragraph 110 shall be submitted to the National Bank of Moldova by its governing body/member or the person authorised by law (showing that the person is authorised to represent the applicant in its relations with the National Bank of Moldova).

115. Within 30 days from the date of receipt of the complete set of documents in accordance with paragraph 110, the National Bank of Moldova shall decide whether to grant an exemption from the obligation to establish the emergency mechanism provided for in paragraph 82 or to reject the application, informing the payment service provider of its decision. The National Bank of Moldova may set, informing the payment service provider, a longer deadline for issuing the decision, which shall not exceed 90 days, under the conditions of the Administrative Code of the Republic of Moldova.

116. If the set of documents submitted to the National Bank of Moldova is not complete and the payment service provider does not submit the documents required for its completion within the deadline set by the National Bank of Moldova, the National Bank of Moldova shall inform the payment service provider about the termination of the administrative procedure within 3 working days from the deadline set by the National Bank of Moldova.

117. If the documents or information submitted in accordance with paragraph 110 are insufficient for the decision to be taken, the National Bank of Moldova may request additional documents and information. The payment service provider shall submit the additional information and documents within the time limit specified by the National Bank of Moldova, during which the time limit set by the National Bank of Moldova under paragraph 115 shall be suspended.

118. The National Bank shall reject the request for exemption from the obligation to establish the emergency mechanism under paragraph 82 if:

a) following the assessment of all documents and information held, the National Bank of Moldova finds that the conditions set out in paragraph 89 are not met and/or the requirements set out in Annex No 3 are not fulfilled; and/or

b) submission to the National Bank of Moldova of erroneous, non-authentic and/or contradictory information and documents.

119. After approval of the exemption from the obligation to establish the emergency mechanism referred to in paragraph 82, the National Bank of Moldova may at any time request from the payment service provider any other information, data, and documents

relevant for the assessment of compliance with the requirements of this Regulation on a continuous basis.

Annex No 1 to the Regulation on strong customer authentication and open, common, and secure standard of communication between payment service providers

	Reference fraud rate (%) for:	
ETV (exemption threshold value)	**Card-based remote electronic payments**	**Remote electronic credit transfer transactions**
MDL 10,000 or the equivalent in foreign currency	0.01	0.005
MDL 5,000 or the equivalent in foreign currency	0.06	0.01
MDL 2,000 or the equivalent in foreign currency	0.13	0.015

Annex No 2 to the Regulation on strong customer authentication and open, common, and secure standard of communication between payment service providers

Application for exemption from the obligation to establish the emergency mechanism under paragraph 89

The undersigned, ... (full name), as . . . . . ., I request exemption from the establishment of the emergency mechanism under paragraph 89 of the Regulation of . . . . . (name of the payment service provider offering online accessible payment account management services), with registered office in . . . . . Str., No . . . . ., postal code . . . . . ., registered at. . . . . ., unique identification code . . . . . for the specific interface . . . . . (name of the specific interface used by the requesting payment service provider).

The specific interface is:

- ☐ internally developed
- ☐ developed within the financial-bank group to which the requesting payment service provider belongs

☐ developed in collaboration with a third-party bank
☐ developed in collaboration with a non-bank third party
☐ purchased from. . . . . (name of the interface manufacturer), with registered office in. . . . . ., ... Str., No . . . . . , postal code. . . . . ., registered at. . . . . ., unique identification code. . . . . .

The software dedicated to the specific interface runs at. . . . . .

The applicant payment service provider is/is not an affiliate or member of a financial/bank group.

The specific interface is/will be used by the following payment service providers:
1. . . . . ., with identification code. . . . . ., in (country). . . . . ., under brand. . . . . .
2. . . . . ., with identification code. . . . . ., in (country). . . . . ., under brand. . . . . .
...
n. . . . . ., with identification code. . . . . ., in (country). . . . . ., under brand. . . . . .

The following documents are annexed to the application:
1. . . . . .
2.
...
n. . . . . .

The contact persons who can provide clarification on this application are:
1. Surname and Given name . . . . . .
Telephone: . . . . . Email: . . . . . .
2. Surname and Given name. . . . . .
Telephone: . . . . . Email: . . . . . .

The data and information provided are true, correct and reflect the situation existing (up to) the date of . . . ./ . . . ./ . . . . .

Signature

Annex No 3 to the Regulation on strong customer authentication and open, common, and secure standard of communication between payment service providers

Requirements for granting exemption from the obligation to establish the emergency mechanism

1. The applicant shall define key performance indicators and service level targets, including for troubleshooting, out-of-hours support, monitoring, contingency plans, and maintenance of the specific interface, which are at least as stringent as those for the

interface(s) made available to its own payment service users for direct online access to their payment accounts.

2. The applicant shall define at least the following key performance indicators for the availability of the specific interface:

1) daily availability of each interface, and

2) daily unavailability of each interface.

3. In addition to the key indicators set out in paragraph 2 of this Annex, the applicant shall define at least the following key performance indicators related to the performance of the specific interface:

1) average daily duration (expressed in milliseconds) per request required for the applicant to provide the payment initiation service provider with all the information required in accordance with Article 52^2 paragraph (4) letter b) of Law No 114/2012 and paragraph 101 subparagraph 2) of this Regulation,

2) average daily duration (expressed in milliseconds) per request required for the applicant to provide the account information service provider with all the information required in accordance with paragraph 101 subparagraph 1) of this Regulation,

3) average daily duration (in milliseconds) per request required for the applicant to provide the card issuer or payment initiation service provider with a "yes" or "no" confirmation in accordance with Article 52^1 paragraph (3) of Law No 114/2012 and paragraph 101 subparagraph 3) of this Regulation,

4) daily rate of erroneous replies.

4. For the purpose of calculating the specific interface availability indicators set out in paragraph 2) of this Annex, the applicant shall:

1) calculate the availability duration expressed in percentages as 100 % minus the percentage of the unavailability duration,

2) calculate the percentage unavailability duration using the total number of seconds that the specific interface was unavailable in a 24-hour period beginning and ending at midnight

3) consider the interface unavailable when five consecutive requests for access to information for the provision of payment initiation services, account information services or confirmation of funds availability have not been answered within a total of 30 seconds, regardless of whether such requests originate from one or more payment initiation service providers, account information service providers or payment service providers issuing card-based payment instruments. In this case, the applicant shall calculate the duration of unavailability from the moment of receipt of the first request in the series of five consecutive requests to which no response was received within 30 seconds, provided that there is no successfully resolved request among the five requests answered.

5. For the purposes of paragraphs 80 and 81 of the Regulation, the applicant shall provide the National Bank of Moldova with a plan for the quarterly publication of daily statistics on the availability and performance of the specific interface, as set out in paragraphs 2 and 3 of this Annex, and of each of the interfaces made available to its payment service users for direct online access to their payment accounts, together with information on the location of the publication of these statistics and the date of first publication.

6. The publication of the statistics referred to in paragraph 5 of this Annex shall enable payment initiation service providers, account information service providers, payment service providers issuing card-based payment instruments to payment service users and competent authorities on a daily basis to compare the daily availability and performance of each specific interface provided by the payment service provider requesting the exception with the availability and performance of each of the interfaces made available to their own payment service users by the same payment service provider for direct online access to payment accounts.

7. For the purposes of the stress tests referred to in paragraph 77 of this Regulation, the applicant shall have processes in place to determine and assess the behaviour of the

specific interface when it is subject to an extremely high number of requests from payment initiation service providers, account information service providers and payment service providers issuing card-based payment instruments, in terms of the impact of such overloads on the availability and performance of the specific interface and on the defined service level objectives.

8. The applicant shall perform appropriate stress testing of the specific interface including, but not limited to:

1) the ability to allow access to multiple payment initiation service providers, account information service providers, and payment service providers issuing card-based payment instruments,

2) the ability to cope with an extremely high number of requests from payment initiation service providers, account information service providers and payment service providers issuing card-based payment instruments in a short time without failures and/or breakdowns,

3) the use of an extremely high number of concurrent/concomitant sessions open at the same time for requests for payment initiation, account information and confirmation of funds availability; and

4) requests involving large volumes of data.

9. The applicant shall provide the National Bank of Moldova with a summary of all stress test results, including the scenarios used as a basis for testing each of the features in paragraph 8 of this Attachment and the manner in which any issues identified have been addressed.

10. The applicant shall provide to the National Bank of Moldova:

1) a summary of the method(s) of implementation of the strict authentication procedure(s) for payment service users supported by the specific interface, i.e., "redirection", "decoupling", "embedding" or a combination thereof; and

2) a clear, detailed and full explanation of the reason why the method(s) of applying the authentication procedure(s) referred to in subparagraph (1) is/are not an obstacle, as provided for in paragraphs 78 and 79 of this Regulation, and the manner in which those methods enable payment initiation service providers and account information service providers to rely on all authentication procedures provided to their own payment service users by the payment service provider requesting the exception, together with the proof that the specific interface does not cause unnecessary delays or inconvenience in terms of the experience generated for payment service users when they access their account through a payment initiation service provider, account information service provider, or payment service provider issuing card-based payment instruments or any other inconvenience, including unnecessary steps or the use of unclear or discouraging language, which may directly or indirectly discourage payment service users from using the services of payment initiation service providers, account information service providers and payment service providers issuing card-based payment instruments.

11. As part of the explanation set out in paragraph 10 subparagraph 2) of this Annex, the applicant shall provide the National Bank of Moldova with a confirmation that:

1) the specific interface does not prevent payment initiation service providers and account information service providers from relying on the authentication procedure(s) provided or offered to their own payment service users by the applicant,

2) no additional licensing or registration is required from payment initiation service providers, account information service providers and payment service providers issuing card-based payment instruments other than those required under Chapter III, Section 1 of Law No 114/2012,

3) no additional checking, as required by paragraphs 78 and 79 of the Regulation, are made by the applicant on the payment service user's consent given to the payment initiation service provider or account information service provider to access information on payment accounts held with the applicant or to initiate payments from payment accounts held with the applicant; and

4) no checking is made of the payment service user's consent given to the payment service provider issuing card-based payment instruments in accordance with Article 52[1] paragraph (2) letter a) of Law No 114/2012.

12. For the purpose of demonstrating compliance with the requirement laid down in paragraph 89 subparagraph 2) of this Regulation, regarding the design of the specific interface, the applicant shall provide the National Bank of Moldova:

1) proof that the specific interface complies with the legal requirements on access and data set out in Law No 114/2012 and this Regulation, including:

a) a description of the functional and technical specifications that the payment service provider has implemented; and

b) a summary of how the implementation of these specifications meets the requirements of Law No 114/2012 and this Regulation,

2) information describing whether and how the payment service provider requesting the exception has interacted with payment initiation service providers, account information service providers and payment service providers issuing card-based payment instruments.

13. In case the applicant implements a standard developed through a market initiative:

1) information referred to in paragraph 12 subparagraph (1) letter a) of this Annex may consist of information on the market initiative standard the applicant is implementing, whether or not the applicant has deviated in any specific respect from such standard, and if so, how it has deviated and how it complies with the requirements of Law No 114/2012 and this Regulation,

2) information referred to in paragraph 12 subparagraph 1) letter b) of this Attachment may include, if available, the results of compliance tests developed by the market initiative, which results attest the compliance of the specific interface with the respective standard of the market initiative.

14. For the purposes of the requirement set out in paragraph 89 subparagraph 2) of this Regulation, in respect of specific interface testing, the applicant shall make the technical specifications of the specific interface available to authorised payment initiation service providers, account information service providers and payment service providers issuing card-based payment instruments or entities that have submitted an application to the National Bank of Moldova for the relevant authorisation in accordance with paragraphs 65-67 of this Regulation, which shall include, as a minimum, the publication of a summary of the technical specifications of the specific interface on its website in accordance with paragraphs 65-66 of this Regulation.

15. The test platform shall allow payment service providers offering account management services, payment initiation service providers, account information service providers and payment service providers issuing authorised card-based payment instruments and entities that have applied to the National Bank of Moldova for the relevant authorisation to test the specific interface in a dedicated testing environment, secure, and with fictitious data of payment service users, for the following:

1) a stable and secure connection,

2) the ability of the applicant and authorised payment initiation service providers, account information service providers and payment service providers issuing card-based payment instruments to exchange the relevant certificates in accordance with paragraphs 91-94 of this Regulation,

3) the ability to send and receive error messages, in accordance with paragraphs 102 and 103 of this Regulation,

4) the ability of the payment initiation service providers to send and the applicant to receive payment initiation orders and the ability of the applicant to provide the required information, in accordance with Article 52[2] paragraph (4) letter b) of Law No 114/2012 and paragraph 101 subparagraph 2) of this Regulation,

5) the ability of account information service providers to send and the applicant to receive requests for access to payment account data and the ability of the applicant to

provide the information requested in accordance with paragraph 101 subparagraph 1) of this Regulation,

6) the ability of payment service providers issuing card-based payment instruments and payment initiation service providers to transmit and of the applicant to receive requests from payment service providers issuing card-based payment instruments and payment initiation service providers and the ability of the applicant to send a “yes” or “no” confirmation to payment service providers issuing card-based payment instruments and payment initiation service providers, in accordance with paragraph 101 subparagraph 3) of this Regulation, and

7) the ability of payment initiation service providers and account information service providers to rely on authentication procedures provided by the applicant to its own payment service users.

16. The applicant shall provide the National Bank of Moldova with a summary of the results of the testing referred to in paragraphs 71 and 72 of this Regulation for each of the elements to be tested in accordance with paragraph 15 of this Annex, including the number of payment initiation service providers, account information service providers and payment service providers issuing card-based payment instruments that have used the testing platform, the response received by the applicant from these payment initiation service providers, account information service providers and payment service providers issuing card-based payment instruments, the problems identified and a description of how these problems have been managed.

17. For the purpose of demonstrating compliance with the requirement of paragraph 89 subparagraph 3) of this Regulation, the applicant shall provide the National Bank of Moldova:

1) a description of the use of the specific interface for the period referred to in paragraph 89 subparagraph 3) of this Regulation, including but not limited to:

a) the number of payment initiation service providers, account information service providers and payment service providers issuing card-based payment instruments that used the interface to provide services to customers; and

b) the number of requests sent by these payment initiation service providers, account information service providers and payment service providers issuing card-based payment instruments to the applicant through the specific interface to which a response was received from the applicant,

2) proof that the applicant has made all reasonable efforts to ensure widespread use of the specific interface, including by communicating the availability of the specific interface through appropriate channels, including, where appropriate, on the applicant's website, social media platforms, industry bodies, at conferences, and through direct engagement with known market players.

18. The three-month period referred to in paragraph 76 subparagraph (3) may run concurrently with the testing referred to in paragraph 58.

19. For the purposes of paragraph 76 and paragraph 89 subparagraph 4) of this Regulation, the applicant shall provide to the National Bank of Moldova:

1) information on the systems or procedures in place for tracking, resolving, and closing problems, in particular those reported by payment initiation service providers, account information service providers and payment service providers issuing card-based payment instruments; and

2) a breakdown of problems and deficiencies, in particular those reported by payment initiation service providers, account information service providers and payment service providers issuing card-based payment instruments, which have not been resolved in accordance with the service level objectives set out in paragraph 1 of this Annex.