Notice: *The translation of the Rule is not of the same legal force as the enacted document in Georgian. The translation has been prepared by the National Bank of Georgia to assist interested parties and serves as a reference tool.*

You can find the official document in Georgian at the website of the Legislative Herald of Georgia and at the website of the National Bank of Georgia.

Order № 156/04

Of the President of the National Bank of Georgia

02/09/2020
City of Tbilisi

On Approval of the Rule on Strong Customer Authentication

On the basis of Paragraph 1(g) of Article 15 and Article 48^2 of the Organic Law of Georgia on the National Bank of Georgia, and Paragraph 5 of Article 30 and the Paragraphs 1, 2(a) and 2(b) of Article 42 of the Law of Georgia on Payment Systems and Payment Services, I order:

Article 1

This Rule on Strong Customer Authentication along with the attached Annex shall be approved.

Article 2

This Ordinance shall come into force upon its publication.

President of the National Bank **Koba Gvenetadze**

Rule on Strong Customer Authentication

Chapter I
General Provisions

Article 1. Purpose and scope

1. The purpose of this Rule is to ensure the secure authentication of payment service users, as well as to protect the confidentiality and integrity of their personalised security credentials, also, to reduce the risk of fraud and of other illegal activities. This will have a positive effect on the stability of the financial sector, strengthen user protection and promote the efficient and reliable functioning of the financial system and payment system, as well as increase confidence of users in payment services and cashless payments.

2. This Rule defines the issues on and pertaining to the implementation of strong customer authentication by the commercial banks licenced by the National Bank of Georgia, payment service providers and microfinance organisations registered by the National Bank of Georgia (hereinafter – the payment service provider). This Rule also defines issues on and related to the exemptions from the requirement to use strong customer authentication and protection of the confidentiality and integrity of personalised security credentials of the payment service users (hereinafter – "user").

3. The scope of this Rule applies where the payer:

a) Accesses his payment account remotely in online regime;

b) Initiates an electronic payment transaction;

c) Undertakes any such action via a remote channel, that carries the risk of fraud and/or other illegal activity.

Article 2. Terms and definitions

The terms used in this Rule have the following meaning:

a) **authentication** – a procedure which allows the payment service provider to verify the identity of a Payment Service User and/or the validity of the use of a specific payment instrument, including the checking personalised security credentials used by the user;

b) **strong customer authentication** – an authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent in a way, that the breach of one in any manner does not compromise the reliability of the other/s. The

procedures of authentication shall designed in such a way to protect the confidentiality of the authentication data;

c) **personalised security credentials** – personalised features provided by the payment service provider to a user for the purposes of authentication;

d) **sensitive payment data** – data, including personalised security credentials, which can be used to conduct a fraudulent transaction;

e) **Batch file** – a set of more than one individual payment operations.

Article 3. General rights and obligations

1. The payment service provider shall ensure strong customer authentication in line with this Rule, when its user - payer:

a) Accesses his payment account remotely in online regime;

b) Initiates an electronic payment transaction;

c) Undertakes any such action through a remote channel, that carries the risk of fraud and/or other illegal activity.

2. The payment service provider is obliged to have a payment transaction monitoring mechanism, with which the payment service provider will be able to identify unauthorised and/or fraudulent payment transactions. The payment service provider is obliged to carry out a real time monitoring of payment transactions when it makes use of the exemptions stipulated in the Article 20 of this Rule, as well as when processing such payment transaction that is executed instantly.

3. The payment transaction monitoring mechanism should be based on an analysis of payment transactions. This analysis should take into account the factors that are characteristic for user, as per the normal/usual use of personalised security credentials by him.

4. The payment service provider is obliged to ensure that the payment transactions monitoring mechanism takes into account at least the following risk-based factors:

a) A list of compromised and/or stolen authentication elements;

b) The amount of each payment transaction;

c) Known fraudulent scenarios that may occur during the provision of a payment service;

d) Signs of existence of such hidden software [malware] in each session of the authentication process, that might cause obstruction and/or corruption, also that is intended for gaining unauthorised access to information;

e) If the technical device or software for accessing is provided to the user by the payment service provider, the records of the usage by the user, including any activity of unusual use.

5. If the payment service provider implements strong customer authentication for accessing a payment account remotely in online regime by user using elements from the knowledge and possession categories, and within the same continuous session the user executes activities prescribed in subparagraphs (b) and (c) of paragraph 1 of this article, then the payment service provider is entitled to reuse the element from the knowledge category, that has been used at the beginning of the session, as one of the elements for strong customer authentication. The payment service provider shall exercise this authority on a risk-based approach.

Article 4. Specific and limited usage payment instruments

1. With the consent of the National Bank of Georgia, a payment service provider is entitled not to apply this Rule to specific, limited usage payment instruments that are valid only in Georgia, and meet one of the following criteria:

a) Within the framework of a commercial/trade agreement concluded immediately between the issuer of instrument and service providers, the owner of such instrument has the opportunity to purchase goods and/or services within the limited network of these service providers;

b) The instrument may only be used to purchase a strictly limited range of goods and/or services;

c) The payment instrument is issued at the request of an entrepreneurial/business entity or an administrative body, serves the social or tax purposes of the administrative body and is used to purchase specific goods and/or services from suppliers who have a contract with the issuer of this instrument.

2. A payment service provider, who intends to use the authority specified in paragraph 1 of this Article with respect to a particular instrument, shall be obliged to submit a written request to the National Bank of Georgia for acquiring consent, providing a description and information about the payment instrument. The National Bank of Georgia shall make a decision on the exercise of this authority by the payment service provide, within 30 working days after receiving the information and description.

Article 5. Verification of security measures

1. A payment service provider shall document the implementation of security measures specified in this Rule and conduct periodical tests, evaluations and audits at least once a year, in accordance with its own established rules. The audit report shall include an evaluation and a report on the compliance of the security measures of the payment service provider with the requirements established by this Rule.

1^1. A payment service providers shall ensure updating the security measures implemented pursuant to this rule in due time based on revealed threats and identified deficiencies from cases realized in practice, test and evaluation, also, based on audit report.

2. The audit referred to in paragraph 1 of this Article shall be carried out by auditor who, regardless of being an employee of the particular payment service provider, is operationally independently from that provider and has the relevant knowledge and experience in the areas of payment services and security of information technologies.

3. A payment service provider, which enjoys the exemption provided in Article 20 of this Rule, shall be obliged to audit the model and methodology, as well as reported (notified) fraud rates, at least on a yearly basis. Such an audit shall include an evaluation of the completeness and accuracy of these rates and data/figures. The requirements of paragraph 2 of this Article shall apply to the auditor.

4. The National Bank of Georgia is authorised to request a payment service provider to conduct an external audit of certain components defined by this Rule. The National Bank of Georgia sets deadline for the conduct of such an audit and the submission of an audit report.

5. In the case of using the exemption provided in Article 20 of this Rule, within one year and at least once every 3 years from the point of starting using these exemptions, or at a higher frequency if so requested by the National Bank of Georgia, the payment service provider is obliged to conduct an external audit of the model and methodology, as well as reported (notified) fraud rates by an independent and qualified auditor/auditors. Such an audit shall also include an evaluation of the completeness and accuracy of the rates and data.

6. The National Bank of Georgia is authorised to request the submission of any full audit report and a payment service provider upon receipt of such a request is obliged to submit such a report within 14 calendar days.

Chapter II

Security measures for strong customer authentication

Article 6. Authentication code

1. Strong customer authentication implemented by a payment service providers shall result in generation of an authentication code. Strong Customer Authentication shall be based on at least two elements from the following different categories:

a) Knowledge;

b) Possession;

g) Inherence.

2. If an authentication code is used to access a payment account remotely in online regime, to initiate an electronic payment transaction or to perform any such action through this remote channel that carries the risk of fraud and/or other illegal activity, then such a code can only be accepted once for authentication by the payment service provider.

3. For the purposes of paragraphs 1 and 2 of this Article, the payment service provider shall develop and implement security measures that meet the following requirements:

a) Disclosure of the authentication code shall not allow revealing/deriving any information about the elements listed in paragraph 1 of this Article;

b) It shall be impossible to generate a new authentication code, based on a knowledge of previously generated authentication code;

c) It shall be impossible to falsify/forge an authentication code.

4. The authentication carried out by the payment service provider through generation of the authentication code shall include all of the following measures:

a) In case of failure of generation of the code, that was to be used according the purposes of paragraph 2 of this Article for accessing a payment account remotely in online regime, initiating a remote electronic payment transaction, or performing any such action through any remote channel that carries the risk of fraud and/or other illegal activity, then it shall be impossible to identify the incorrect element(s) out of used elements;

b) The maximum number of consecutive failed authentication attempts, as a result of which the actions by the user specified in paragraph 1 of Article 3 of this Rule will be temporary or permanently blocked, for the period of time defined by the provider on the basis of a risk-based approach, shall not exceed 5;

c) Communication sessions shall be protected from unauthorised parties accessing, capturing and manipulating the authentication data transmitted during the authentication process;

d) While accessing a payment account by an authenticated payer remotely in online regime, the maximum uninterrupted period of inactivity shall not exceed 5 minutes. The payment service provider is entitled, on a risk-based approach, to determine this duration for legal entities as no more than 10 minutes.

5. In the case of transactions executed with a card-based instrument, the obligation provided in paragraph 4 (a) of this Article shall apply only in cases where the issuer and the acquirer involved in the operation are a commercial bank licensed by the National Bank of Georgia, and a payment service provider or a microfinance organisation registered by the National Bank of Georgia.

6. If blocking specified in the paragraph 4(b) of this Article:

a) Is temporary, the duration of blocking and number of re-attempts shall be determined based on the characteristics of the service provided to the payer and all relevant risks, that shall take into account at least the factors specified in paragraph 4 of Article 3 of this Rule;

b) Is permanent, a secure procedure shall be developed to ensure that the payer can re-enable the blocked electronic payment instruments and electronic channels for accessing the accounts.

7. Before blocking permanently, the payment service provider is obliged [in advance] to inform a user on this matter.

8. The requirement of paragraph 4(a) of this Article shall not apply to the initiation of a payment transaction through a physical POS terminal and an ATM.

Article 7. Dynamic linking

1. In order to use strong customer authentication when initiating an electronic payment transaction, the payment service provider, in addition to complying with the requirements of Article 6 of this Rule, shall develop and implement security measures that meet all of the following requirements:

a) The payment service provider is obliged to show the payer information about the amount of the transaction and the payee;

b) The authentication code shall be generated specifically for the exact amount and payee of the payment transaction, which were confirmed by the payer while initiating the payment transaction;

c) The authentication code accepted by the payment service provider must correspond to the original amount and payee of the payment transaction confirmed by the payer;

d) Any change in the amount of the payment transaction or the payee, shall result in the invalidation of the generated authentication code.

2. For the purposes of paragraph 1 of this Article, the payment service provider is obliged to develop and implement security measures, through which confidentiality, authenticity/constancy and integrity of the following information shall be ensured:

a) The amount and payee of the payment transaction, at any stage of the authentication;

b) Information provided to the payer at any stage of the authentication process, including the process of generating, transmitting, and using the authentication code.

3. When a payment service provider is using strong customer authentication, for the purposes of paragraph 1(b) of this Article the authentication code shall meet the following requirements:

a) In the case of a card-based payment transaction, for the initiation of which the payer has agreed to block a specified amount, the authentication code shall correspond only to the amount, which was confirmed by the payer and which the payer agreed to be blocked when initiating the payment transaction;

b) In the case of a payment transaction where the payer has agreed to perform a remote electronic payment transaction in the form of a batch file to one or more payees, the authentication code shall only correspond the total amount of the batch file of these payment transactions and specified payee/payees.

Article 8. Requirements for elements of the knowledge category

1. The payment service provider shall develop and implement measures to mitigate the risks of elements of the knowledge category, as defined by paragraph 1 of Article 6 of this Rule, being uncovered by or disclosed to unauthorised persons.

2. The payment service provider shall develop and implement risk mitigation measures to prevent disclosure of knowledge category elements by payers to unauthorised persons.

Article 9. Requirements for elements of the possession category

1. The payment service provider shall develop and implement measures to mitigate the risks of elements of the possession category, as defined by paragraph 1 of Article 6 of this Rule, being used by unauthorised persons.

2. The payment service provider shall develop and implement measures to prevent the replication of possession elements.

Article 10. Requirements for elements of the inherence category

1. The payment service provider is obliged to develop and implement measures to mitigate the risks of such elements of the inherence category (defined by paragraph 1 of Article 6 of this Rule) that are read by technical device and software provided to the payer, being uncover by unauthorised persons.

2. The payment service provider, at a minimum, shall ensure that there is a significantly low probability of an unauthorised person being authenticated as a payer by the devices and software referred to in paragraph 1 of this Article.

3. The payment service provider is obliged to develop and implement measures for the elements used by user referred to in paragraph 1 of this Article. These measures shall prevents unauthorised use of these elements through unauthorised access to devices and software.

Article 11. Independence of the elements

1. The payment service provider is obliged to develop and implement measures for the use of strong customer authentication elements in terms of technology, algorithms and parameters,

so that compromising of one of the elements does not result in compromising the reliability of other elements.

2. The payment service provider is obliged to develop and implement security measures in the case any element of strong customer authentication or authentication code is used through a multi-functional technical device, in order to mitigate the risks arising from compromising of such device.

3. The measures referred to in paragraph 2 of this Article shall include all of the following:

a) The use of separated secure execution environments through the software installed in the multi-functional technical device;

b) Mechanisms to assure the provider that the device or the software provided to the user has not been modified/altered by the payer, or a third party;

c) If a device or software provided to user has undergone modification/alteration – mechanisms for mitigating consequences of the mentioned.

Chapter III

Exemptions from the requirement of strong customer authentication

Article 12. Information on payment accounts

1. The payment service provider is entitled, in compliance with the requirements of paragraph 2 of this Article and paragraphs 2 through 4 of Article 3 of this Rule, to be exempted from the requirement to use strong customer authentication, if the user has remote/online access only to one or both of the following information (excluding any sensitive payment data):

a) The balance of one or more payment accounts specified/designated by the user;

b) Information on payment transaction executed during the past 90 calendar days, via one or more payment accounts specified/designated by the user.

2. The authority specified in paragraph 1 of this Article does not apply and the payment service provider shall carry out strong customer authentication, if at least one of the following conditions is met:

a) The user attempts remote access to the information in online regime, as specified in paragraph 1 of this Article, for the first time;

b) More than 90 calendar days have elapsed since the last remote access to information in online regime by the user, as specified in paragraph 1(b) of this Article, and the fulfilment of the last strong customer authentication request.

3. The payment service provider, within the scope of exempted use in accordance with this Article, is entitled to not apply the requirement of paragraph 4(d) of Article 6 of this Rule, with

respect to a request for information about an account balance and/or execute payment transactions.

4. If access to the information referred to in paragraph 1(b) of this Article is exercised only by using the knowledge category element, the payment service provider is entitled to use this element of the knowledge category for strong customer authentication for accessing to transactions of more than 90 days within the same continuous session, .

Article 13. Contactless payments in retail/service Outlets

1. The payment service provider is authorised, in compliance with the requirements of paragraphs 2 through 4 of Article 3 of this Rule, to not use strong customer authentication if the user initiates a contactless electronic payment transaction, and one of the following provisions is satisfied:

a) The amount of one contactless transaction shall not exceed 150 GEL, or its equivalent in foreign currency, and the maximum amount of contactless payments made consecutively shall not exceed 600 GEL, or its equivalent in foreign currency;

b) The amount of one contactless transaction shall not exceed 150 GEL, or its equivalent in foreign currency, and the maximum number of contactless payments made consecutively shall not exceed 4 payments.

Article 14. Self-service terminals [intended] for the payment of transport fares and parking fees

1. The payment service provider is entitled, in compliance with the requirements of paragraphs 2 through 4 of Article 3 of this Rule, not to use strong customer authentication if the payer initiates an electronic payment transactions at self-service terminals specifically [intended] for the payment of such transportation fares and parking fees, amount of which is fixed and cannot be changed by the user.

Article 15. List of trusted beneficiaries

1. The payment service provider is obliged to use strong customer authentication if the payer creates, or changes a list of trusted beneficiaries through the payer's account servicing payment service provider.

2. The payment service provider is entitled, in compliance with the requirements of paragraphs 2 through 4 of Article 3 of this Rule, not to use strong customer authentication if the payer initiates a payment transaction and the payee was added to the list of trusted beneficiaries prior to this activity [initiation]. The use of this exception is only allowed 24 hours after the payer has added the payee to the list of trusted beneficiaries.

3. For the purposes of this Article, a trusted beneficiary is a payee whom the user has trust in, and the execution of a payment transaction in their favour, without the use of strong customer authentication, in the payer's view has no risk. The payment service provider is obliged to provide the user with clear and detailed information about the mentioned.

4. The payment service provider is entitled to determine the beneficiaries, both through a risk-based approach, as well as complaints received from customers, in relation to which the payment service provider will not exercise the exception provided for in this Article.

5. The payment service provider does not have the right to consider the saving of a payee's account details by the user as adding the payee to the list of trusted beneficiaries.

Article 16. Recurring/periodic payment transactions

1. The payment service provider is obliged to use strong customer authentication if the payer creates, changes or for the first time initiates a series of recurring/periodic payment transactions.

2. The payment service provider is entitled, in compliance with the requirements of paragraphs 2 through 4 of Article 3 of this Rule, not to use strong customer authentication to initiate all subsequent payment transactions within a series, as referred to in paragraph 1 of this Article, if the amount of the recurring/periodic payment transaction and the payee remain the same.

3. If the service specified in paragraph 2 of this Article involves a payment transaction through conversion of the same amount in favour of the same Payee, the payment service provider shall notify the exchange rate to the user, before strong customer authentication as specified in paragraph 1 of this Article.

4. The payment service provider is entitled, in compliance with the requirements of paragraphs 2 through 4 of Article 3 of this Rule, not to use strong customer authentication to initiate all consecutive payment transactions within a series, as referred to in paragraph 1 of this Article, if the payee remains the same and the user has explicitly defined the principle of calculating the amount of transactions to be executed.

Article 17. Credit transfer between accounts of the same user

1. The payment service provider is entitled, in compliance with the requirements of paragraphs 2 through 4 of Article 3 of this Rule, not to use strong customer authentication if the payer initiates a credit transfer, where the payer and the payee are the same person, and the he holds the both payment accounts within the same account servicing payment service provider.

2. The payment service provider is entitled to make use of the exception defined in this article in the case where the user has accessed his account only with knowledge or inherence category element. The payment service provider shall exercise this authority according to a risk-based approach.

Article 18. Law-value payment transaction

1. The payment service provider is entitled not to use strong customer authentication if the payer initiates a remote electronic payment transaction, the amount of which does not exceed 50 GEL, or its equivalent in foreign currency, and one of the following provisions are fulfilled:

a) The total value of remote electronic payment transactions initiated by the payer, since the last execution of strong customer authentication, does not exceed 250 GEL, or its equivalent in foreign currency;

b) The number of individual consecutively initiated remote electronic payment transactions by the payer, since the last execution of Strong Customer Authentication, has not exceeded five.

Article 19. Security processes and protocol used by legal entities

The payment service provider is entitled not to use the strong customer authentication with legal entities that initiate electronic payment transactions through such special payment processes or protocol, which ensure at least the same extent/level of security as required by this Rule.

Article 20. Payment transactions risk analysis

1. The payment service provider is entitled not to use strong customer authentication, if the payer initiates a remote electronic payment transaction which is identified as low risk by the payment service provider according to the payment transaction monitoring mechanism referred to in paragraph 2(c) of this Article and of Article 3 of this Rule.

2. An electronic payment transaction referred to in paragraph 1 of this Article shall be deemed to be of a low risk, if the following provisions are complied with:

a) The fraud rate reported (notified) by, and calculated by the payment service provider in accordance with Article 21 of this Rule, shall not exceed the rate specified in columns of “remote electronic card-based payments” and “remote electronic credit transfers”, in the Annex of this Rule;

b) The amount of the payment transaction does not exceed the upper limit of the amount, for the use of the exemption, specified in the Annex to this Rule,;

c) As a result of real-time risk analysis carried out by the payment service provider, the following were not detected/identified:

c.a) Unusual spending and behavioural pattern of the payer;

c.b) Unusual information concerning the access to payer's technical device or software;

c.c) The existence of hidden software [malware] that might cause obstruction and/or corruption, also that is intended for gaining unauthorised access to information, in any of the sessions of authentication;

c.d) Known payment service fraud scenarios;

c.e) Unusual location of the payer;

c.f) High-risk location of the payee.

3. A payment service provider, which on the basis of the low risk of payment transactions plans to exempt such transaction from the requirement of strong customer authentication, is obliged to take into account at least the following risk-based factors:

a) The characteristic spending pattern of a particular payment service user;

b) The payment transactions history of each user of the payment service provider;

c) If the technical device or software for access is provided by the payment service provider, the location of the payer and payee at the time of the payment transaction;

d) Detection of an unusual pattern of payment by the user, in relation to the history of payment transactions of the same user.

4. The assessment of transactions, as specified in paragraph 3 of this Article, shall be carried out by the payment service provider on the basis of the level of risk (score), calculated for each individual transaction, and taking into account all the factors specified in paragraph 3 of this Article.

Article 21. Calculation of fraud rates

1. The payment service provider is obliged to calculate the fraud rates.

2. For each type of payment transaction specified in the Annex to this Rule, the fraud rate, which includes both payment transactions performed in compliance with the requirements of strong customer authentication, as well as payment transactions executed using the exemptions provided for in Articles 15 through 20 of this Rule, shall not exceed the fraud rate specified in the Annex to this Rule, for the same/corresponding type of payment transaction.

3. The fraud rate for each type of payment transaction specified in the Annex to this Rule shall be calculated quarterly, as the total value of unauthorised and/or fraudulent remote payment transactions, regardless of whether the refund was made, divided by the total value of the same type of remote payment transaction. The calculation shall take into account the transactions executed in compliance with the requirements of strong customer authentication, as well as the exempted transactions stipulated by Articles 15 through 20 of this Rule.

4. The methodology and any model used by the payment service provider to calculate the fraud rate, as well as the result fraud rates shall be documented in detail and

clearly/accurately. Upon the request of the National Bank of Georgia, the payment service provider is obliged to submit the above-mentioned documentation to the National Bank of Georgia.

Article 22. Cessation of use of the exemption

1. If the fraud rates calculated in connection with any type of payment transaction, which are specified in [a table in] the Annex to this Rule and are monitored by the Payment Service Provider, exceed the relevant rates specified in the same table, then a payment service provider which uses the exemption referred to in Article 20 of this Rule, is obliged to immediately notify the National Bank of Georgia on this matter.

2. The payment service provider is obliged to provide the National Bank of Georgia with a description of the measures it plans to implement, in order to restore compliance with the rates referred to in the table.

3. The payment service provider is obliged to immediately cease the use of the exemptions provided in Article 20 of this Rule, in relation to any type of payment transaction within the limits of the corresponding amount of the transaction specified in the Annex to this Rule, if the fraud rate monitored during] two consecutive quarters exceeded the fraud rate set for the relevant type and amount of payment transaction.

4. After the cessation of use of the exemption, in accordance with paragraph 3 of this Article, the payment service provider is be entitled to use the exemption again, if the calculated fraud rate for a particular type of payment transaction, within the relevant marginal/limit amount during one quarter, did not exceed the fraud rate specified in the Annex to this Rule.

5. If the payment service provider plans to again use the exemptions referred to in Article 20 of this Rule, it shall notify the National Bank of Georgia, 10 calendar days in advance and provide information confirming the compliance of the monitored fraud rate with the rate specified by this Rule.

Article 23. Monitoring

1. In order to use the exemptions provided in Articles 12 through 20 of this Rule, the payment service provider is required to carry out recording and monitoring of the following data for all types of payment transaction, with a breakdown for remote and non-remote payment transactions, at least on a quarterly basis:

a) The total value of unauthorised and fraudulent payment transactions, as well as the total value of all payment transactions, and the calculated fraud rate, including transactions executed with fulfilment of the requirements of strong customer authentication and transactions executed using each exemption;

b) The average value of payment transactions, including those executed with fulfilment of the requirements of strong customer authentication and transactions executed using each exemption;

c) The number of payment transactions executed using an exemption and the percentage of such transactions in the total number of payment transactions, according to the type of exemption.

2. At the request of the National Bank of Georgia, the payment service provider is obliged to submit the results of the monitoring carried out in accordance with paragraph 1 of this Article, to the National Bank of Georgia.

Chapter IV

Protecting the confidentiality and integrity of user's personalised security credentials

Article 24. General requirements

1. The payment service provider shall ensure the confidentiality and integrity of the personalised security credentials of the user at all stages of authentication, including the privacy and integrity of the authentication codes.

2. For the purposes of paragraph 1 of this Article, the payment service provider shall ensure that each of the following requirements is met:

a) personalised security credentials shall be masked and not readable in their full extent when input by the user, during the authentication;

b) personalised security credentials in a data format, as well as cryptographic material related to the encryption of the personalised security credentials, shall not be stored in an unencrypted text format;

c) Secret cryptographic material is protected from unauthorised disclosure.

3. The payment service provider is obliged to ensure full documentation of the process of managing cryptographic material used for the encryption of personalized security credentials or their otherwise unreadable render.

4. The payment service provider shall ensure processing and transmission of personalised security credentials and authentication codes, generated in accordance with Chapter II of this Rule, in accordance with strong and widely recognised standards.

Article 25. Creation and transmission of personalised security credentials

1. The payment service provider is obliged to ensure the creation of personalised security credentials in a secure environment.

2. The payment service provider is obliged to ensure mitigating the risks of the unauthorised use of personalised security credentials, authentication devices and software, which was resulted from their loss, theft, or copying prior to delivery to the payer.

Article 26. Association with payment service users

1. The payment service provider is obliged to ensure association of only one user with personalised security credentials, authentication devices and software, in a secure way.

2. For the purposes of paragraph 1 of this Article, the payment service provider shall ensure that each of the following requirements are met:

a) The association of the user with personalised security credentials, authentication devices and software shall be carried out in a secure environment, which is under the responsibility of the payment service provider. At a minimum, this [secure environment] includes the payment service provider's offices, an internet environment, or other similarly secure websites, and its ATM system and also takes into account the risks associated with technical devices and other components used in the association process, that are not its responsibility;

b) The association of the user with personalised security credentials, authentication devices and software through a remote channel shall be carried out using strong customer authentication.

Article 27. Delivery of personalised security credentials, authentication devices and software

1. The payment service provider is obliged to provide personalised security credentials, authentication devices and software to the user in a secure manner, thus ensuring that the risks of their unauthorised use caused by their loss, theft or copying are mitigated.

2. For the purposes of the paragraph 1 of this Article, the payment service provider is obliged to develop and implement, at a minimum, the following mechanisms and measures:

a) Effective and safe delivery mechanisms that ensure the delivery of personalised security credentials, authentication devices and software payment services to authorised users;

b) Mechanisms that enable the payment service provider to verify the authenticity/constancy of the authentication software provided to the user via the internet;

c) Measures for the cases where personalised security credentials are not provided in the offices of the payment service provider, or [such provision/delivery] is carried out via a remote channel, and at the same time, the following requirements are met:

c.a) If the delivery is made through the same channel, no unauthorised party may obtain more than one feature/parameter of personalised security credentials, authentication device or software;

c.b) That the provided personalised security credentials, authentication devices or software require activation before use.

d) In the case, activation is required before the first use of personalised security credentials, authentication devices or software, the activation process is executed in a secure environment, in compliance with the requirements of Article 26 of this Rule.

Article 28. Renewal of personalised security credentials

The payment service provider is obliged to ensure the renewal or re-activation of personalised security credentials, in accordance with the requirements specified in the Articles 25 through 27 of this Rule.

Article 29. Destruction, deactivation and revocation

The payment service provider is obliged to ensure effective processes for the implementation of all of the following security measures:

a) The secure destruction, deactivation and/or revocation of personalised security credentials, authentication devices and software;

b) If the payment service provider provides already used authentication devices and software, it is obliged to develop, document and implement measures for their secure re-use before transferring them to other users;

c) Deactivation or revocation of information related to the personalised security credentials stored in the payment service provider's own and/or outsourced systems and databases.

Chapter V

Liabilities of the provider

Article 30. Liabilities of the payment service provider

1. If the payer's payment service provider has implemented a strong customer authentication mechanism, and upon its request the payee's payment service provider cannot provide support for strong customer authentication during the payment transaction, then the payee's payment service provider is obliged to refund the payer's payment service provider financial loss, not exceeding the amount of the transaction refunded to the payer. However, if strong authentication support is not provided solely because of the payee, the liability is governed by the contract conducted between the payee and the payee's payment service provider.

Chapter VI

Transitional provisions

Article 31. Transitional provisions

1. With respect to e-commerce transactions executed with card-based instrument:

a) The acquirer is obliged to provide the possibility of using a one-time code as an authentication element, no later than the November 1, 2020;

b) From November 1, 2020, in case of high-risk payees, acquirer is obliged to execute transaction (including the first, as well as subsequent transactions with requisites of saved card-based instrument) on the basis of confirming the transaction with a one-time code by the user, if the issuer has implemented relevant mechanism of one–time code. From January 1, 2021, in case of high-risk payees the issuer and acquirer shall ensure execution of transaction only on the basis of confirmation with a one-time code by the user;

c) The acquirer shall, within the 15 days of the entry into force of this Rule, ensure prior provision of information to users, about the use of one-time codes;

d) The payment service provider (Issuer and Acquirer) is obliged to ensure the execution of e-commerce transactions in compliance with the requirements of this Rule, no later than January 1, 2023.

2. Except for card-based transactions, payment service provider is obliged to ensure access to payment accounts through a remote channel (website or mobile application), and payments made through these channels, are in compliance with this Rule, no later than March 22, 2021.

3. In case of a card-based instruments issued by a foreign country's payment service provider, the [local] payment service provider is entitled to act, on a risk-based approach, until January 1, 2025.

4. Until January 1, 2025, the issuer is entitled to act, on the basis of a risk-based approach, in relation to card-based transactions made by its users at merchant outlets being serviced by a foreign acquirer.

5. After entry into force of this Rule the payment service provider is obliged to issue only such card-based instruments that fully comply with the requirements of this Rule.

6. No later September 1, 2021, the payment service provider is obliged to replace the issued card-based instruments that do not meet the requirements of this Rule, with card-based instruments that fully comply with the requirements of this Rule. In the event that the user's payment instrument has not expired, the issuer is entitled to charge the user for the replacement with a cost of no more than the payment instrument itself.

7. The payment service provider is entitled prior to the implementation of the monitoring mechanisms, as specified in Article 20 of this Rule, for card-based payment transaction - not later than January 1, 2024, and for other payment transactions – not later than January 1,

2023, to assess the risk level of payment transactions, based on existing experience, including user complaints. After the implementation of the monitoring mechanisms, the payment service provider is obliged to reassess the risk level of any payment transaction in accordance with the requirements of this Rule.

8. Before the implementation of the monitoring mechanisms, as specified in Article 20 of this Rule, but not later than January 1, 2023, the payment service provider is entitled, in accordance with the rules established by the legislation of Georgia, and based on a contractual relationship established with the user, as well as with their consent, check their standing debt with household utility companies, based on their subscriber number or other identifier and initiate payment transactions of no more than their amount of debt. The payment service provider is entitled to provide such a service to their users if among possible options the user selected the duration of consent or gave consent for indefinite period of time, and specified the upper limit of the payment amount. In the case prescribed in this paragraph, obligations related to amount of transaction prescribed in Article 20 of this Rule do not apply to monitoring mechanism.

9. A payment service provider, which provides services to their users, as provided for in paragraph 8 of this Article, on the basis of consent obtained before the entry into force of this Rule, and the term of the validity of this consent is not specified, is obliged to ensure the renewal of the relevant consent, of each such user, by March 1, 2021, on the basis of strong authentication. The renewed consent, in accordance with this paragraph, shall include the term of its validity and the upper limit of the amount. This paragraph does not apply where the payer, prior to entry into fore of this Rule, among possible options had selected duration of consent or gave consent for indefinite period.

10. A provider, who offers payment services to users through their website, is entitled to allow the user to attach a payment instrument (card-based and/or other) to the identifier of the user registered on the provider’s e-wallet/website. The attachment of the payment instrument is made, in order to replenish the wallet and/or transfer money from the wallet to the payment instrument, as well as for the purposes of single payment transactions. In the case provided for in this paragraph, except for an instrument issued by a foreign payment service provider, the operation of attaching the payment instrument shall be carried out by the issuer on the basis of strong customer authentication, or the use of a one-time code [in the case that it is] before January 1, 2024. In the case of an identified user, the execution of strong authentication (or the generation of a one-time code) by the issuer is not required when initiating the operation to replenish the wallet, or make a single payment transaction with the payment instrument. In the [above-mentioned] cases, access to the e-wallet or access to the user's data registered on the website shall be based on strong customer authentication by the provider. In the case of unidentified user, when initiating a transaction with a payment instrument from a website, the payment service provider shall require the issuer of the payment instrument to carry out strong authentication or use a one-time code. The responsibility for the transactions performed in violation of this paragraph, before the provider issuing the payment instrument

and the user of the payment instrument, lies with the website service provider (including an e-money provider).

11. Until the January 1, 2025, the payment service provider is authorised not to consider payments of up to 10 GEL when calculating for the purposes of Article 13 of this Rule, if the maximum number of contactless payments executed is limited to 30 per day by the payment service provider.

12. For the purpose of using the right prescribed in Article 13 of this Rule, the provider is obliged no later than the March 1, 2021, to ensure compliance with the obligations defined in the same article in regard to counting maximal value of or number of contactless payments executed subsequently. Before March 1, 2021, contactless payment value executed without strong customer authentication shall not exceed 100 GEL.

13. The payment service provider is obliged to implement a monitoring mechanism for payment transactions no later than January 1, 2022, which will enable it to identify unauthorised and/or fraudulent payment transactions.

14. After January 1, 2023, in order to benefit from the exemptions specified in Articles 12, and 14 through 20 (except for card-based payment transactions) of this Rule, the payment service provider shall be obliged to implement the relevant monitoring mechanism provided for in this Rule, and for making use of exemptions stated in the above-mentioned articles for card-based payment transactions – not later than January 1, 2024.

15. The first audit, specified in paragraphs 1 and 3 of Article 5 of this Rule, shall be carried out no later than May 1, 2023.

16. A payment service provider, who wishes to exercise the authority specified in Article 4 (1) of this Rule, in respect of payment instruments issued before the entry into force of this Rule, shall provide the National Bank of Georgia with a written description and information on such payment instruments, within 30 calendar days after this Rule comes into force. The National Bank of Georgia makes a decision on the exercise of this authority, by the payment service provider, within 60 working days after receiving the written notification. The National Bank of Georgia specifies in the decision a period of time, during which this Rule will not apply to the said payment instrument.

17. In the case of using the provisions in this Article, the payment service provider is obliged to refund the payer the amount of an unauthorised payment transaction, executed without strong customer authentication, as soon as possible, but no later than the end of the next working day after the provider became aware of the unauthorised transaction or has received a notification. The payer's payment service provider is obliged to restore the debited payment account into the situation in which it would have been, had the unauthorised payment transaction without strong customer authentication not taken place. The provider shall not be liable to the payer under this clause of refund, if it has a reasonable suspicion of a fraudulent

act by the user, and the provider has notified the National Bank of Georgia in writing, as well as addressed the relevant law enforcement authority.

18. If this article does not specify otherwise, the payment service provider is obliged to ensure full compliance with the requirements of this Rule, no later than January 1, 2023.

Annex

	Fraud rate (%):	
The marginal value of the transaction for the use of the exemption	**Remote electronic card-based payment**	**Remote electronic credit transfers**
500 GEL	0.01	0.005
250 GEL	0.06	0.01
100 GEL	0.13	0.015