Recommendation No 5/2023 (VI.23.) of the Magyar Nemzeti Bank
on the prevention, detection and management of abuses observed through payment services

I. Purpose and scope of the recommendation

The purpose of the recommendation is to publish the expectations of the Magyar Nemzeti Bank (hereinafter: MNB) with regard to the prevention, detection and management of abuses observed through payment services, to support the application of related laws and to foster the development of standard practices in issues not regulated by the laws.

The recommendation is addressed to the payment service providers specified in point 22 of Article 2 of Act LXXXV of 2009 on the Pursuit of the Business of Payment Services (hereinafter: Payment Services Act) acting as payment institutions, with the exception of the MNB, the Treasury, the institution operating the Clearing Centre of the Hungarian Post and of the construction trustee service providers specified in Government Decree No 191/2009 (IX. 15.) on Building Contractor Activities (hereinafter collectively: payment service provider).

As digitalisation accelerates, significant changes are taking place in all areas of life, and finance is not an exception to this either. On the one hand, the use of smart devices and the internet has become a common trend, and as a result, daily financial transactions also tend to be managed in digital form, largely supported by payment service providers and other service providers (e.g., merchants) as well. On the other hand, remote access to consumers, especially through social media platforms, becomes increasingly easy, opening up new opportunities for fraud.

As regards abuses, two main trends can be observed. One of those is the diversion of previous abuses, based on personal meetings, to electronic channels, where there is no longer a risk of a direct encounter. The other one is the exploitation of modern technologies, which offer many new opportunities for those who want to commit abuses. In the course of this, fraudsters are using more and more sophisticated solutions, increasingly difficult to identify, in their attempts to pilfer customers' money.

In parallel with this, several new forms of abuse appeared in the digital space, all of them having the common feature that they have some impact on electronic payments. Accordingly new types of abuses include frauds based on, among others, obtaining personal authentication and sensitive payment data and then using those data to initiate unauthorised payment orders, as along with abuses based on deception and psychological manipulation – whereby the payer is persuaded to give a payment order, or to approve payment orders submitted by the perpetrators of the abuse – and abuse based on direct access to a payment instrument in the payer's possession, such as a payment card, mobile bank or internet bank.

Considering the fact that as a result of the opportunities provided by technological progress, those committing abuses increasingly target the digital space, and in parallel with that, the electronic payment services. However, this may provide an opportunity as well for using the information generated in the course of the provision of payment services in order to manage the aforementioned risks. This is exactly why payment service providers are required to apply such transaction monitoring mechanisms and take customer education measures that are able to prevent, detect and – as far as possible – block abuses attempted in the course of providing payment services, irrespective of the manner of the attempted abuse.

In this recommendation, the MNB formulates the expected protective measures – and recommended as good practice – aimed at the prevention, detection and blocking of abuses for payment service providers.

The MNB welcomes the application of practices going beyond the expectations of the recommendation, aimed at enhancing customers' security.

Furthermore, the MNB emphasises that it expects payment service providers to comply with the provisions hereof in a way that hinders customers and reduces customer experience to the smallest possible degree in respect of the payment services rendered by the payment service provider – particularly the acceptance of payment orders, the execution of the related strong customer authentication and the processing of payment orders – in the use of payment services, commensurately with the risks.

In the course of developing the recommendation, the MNB took into consideration the provisions of Directive 2015/2366/EU of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation 1093/2010/EU, and repealing Directive 2007/64/EC (hereinafter: PSD2), Commission Delegated Regulation 2018/389/EU of 27 November 2017 Supplementing Directive 2015/2366/EU of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication (hereinafter: SCA Regulation), Act CCXXXVII of 2013 on credit institutions and financial enterprises (hereinafter: Credit Institution Act), Act CCXXXV of 2013 on Certain Payment Service Providers (Payment Service Provider Act), the Payment Services Act and Government Decree No 42/2015 (III. 12.) on protecting the information system of financial institutions, insurance undertakings, reinsurance undertakings, investment firms and commodity dealers (hereinafter: Decree).

In addition to the foregoing, the provisions hereof shall be interpreted jointly with the provisions of the MNB's relevant other recommendations, particularly of MNB Recommendation No 26/2018 (VIII. 16.) on the security measures related to the operational and security risks of payment services, MNB Recommendation No 8/2020 (VI.22.) on the protection of IT systems and MNB Recommendation No 12/2022 (VIII. 11.) on setting up and using internal safeguards and on the management and control functions of financial organisations.

The liability and loss bearing rules, based on PSD2 and specified in the Payment Services Act, have been framed with a view to protecting consumers to a greater extent, since they have a limited ability to enforce their individual interests. In addition to this, payment service providers have the ability to develop their IT systems related to payment services in a way that ensures the highest possible security commensurate with the risks, while their customers have no impact on this. In line with PSD2, the Payment Services Act and the SCA Regulation supplementing PSD2, the MNB expects financial service providers to achieve the highest level of security.

The highest level of consumer protection is of utmost importance for the MNB. The MNB believes that this can be achieved if payment service providers use modern and reliable security systems and procedures, prepared for the identification of known fraud patterns, which are able to prevent potential abuses. The MNB attaches special importance to the application of the "Know your Customer" principle in the monitoring of abuses by payment service providers, as part of which – for example – the payment service provider, if a payment transaction deviating from the customer's payment habits is initiated – in the absence of the authorisation prescribed by Article 37(1) and (2) of the Payment Services Act – the payment service provider either rejects it in line with Article 9(1) of MNB Decree No 35/2017 (XII. 14.) on Payments Services Activities (hereinafter: MNB Decree), or suspends the execution of it based on the provisions of Act LIII of 2017 on the Prevention of and Combating Money Laundering and Terrorist Financing (hereinafter: AML

Act), or disables the payment instrument presumably affected by the abuse pursuant to Article 39(2) of the Payment Services Act.

The risk factors and expected measures described in the recommendation are not comprehensive. Payment service providers are advised to also take into consideration risk factors and measures better fitting their own customers and activities, as necessary.

When formulating the principles and expectations, this recommendation does not make a full reference to the relevant statutory provisions. Nevertheless, the addressees of this recommendation are obliged to comply with the related statutory provisions irrespective of complying with the provisions hereof.

The recommendation does not provide any guidance on data management and data protection issues, does not contain any expectations with regard to the processing of personal data and the requirements contained in this recommendation should not be in any way interpreted as an authorisation to process personal data. Data processing in the context of the fulfilment of the supervisory requirements set out in the recommendation should only be carried out in compliance with the data protection legislation in force at any time.

II. Interpretative provisions

1. For the purposes of this recommendation:
    1. *communication via electronic channels*: a one-way or multi-directional communication solution – other than paper-based solution – that delivers data or information to the customer or payment service provider electronically, such as a push message, short text message (SMS), e-mail, other message sent by the mobile or internet banking application, or as an image and sound or video transmission;
    2. *cross identification*: a method used for customer authentication when establishing customer relationship through telephone or other voice-based instrument supporting direct communication, where part of the answers to the – at least three – questions asked by the representative of the payment service provider is provided by the representative of the payment service provider and other part of those is answered by the customer contacting the provider;
    3. *push message*: electronic message or notification sent to the customer from an application or website.
2. Additional terms used in the recommendation – unless provided otherwise – shall have the meaning defined in the SCA Regulation, the Credit Institutions Act, the Payment Service Providers Act, the Payment Services Act, the AML Act and in the MNB Decree.

III. Provision of information prior to concluding the framework contract and requirements connected to the content elements of the framework contract

3. The MNB reminds the addressees of this recommendation that no deviation is allowed from the binding provisions of Chapter IX of the Payment Services Act concerning the adjustment of payment

transactions, and the liability and loss bearing rules – considering the provisions of Article 34 of the Payment Services Act – to the detriment of consumers or microenterprises. Accordingly, the information prior to concluding the framework contract (hereinafter for the purpose of this Chapter III: information) and the framework contract itself shall not contain any condition as a result of which the authorisation of the payment transactions alone, related to a payment transaction resulting from the unauthorised use of a payment card, mobile banking or internet banking application, would prove the contracting party's gross negligence, since such contractual conditions are in conflict with the provisions of Article 43(2)[1] and Article 45(3)[2] of the Payment Services Act. Accordingly, the payment service provider shall not override or impair the consumer protection provisions of the Payment Services Act and the principle of reasonable conduct specified in Article 1:4 of Act V of 2013 on the Civil Code (Civil Code) in the information provided prior to concluding the framework contract and in the framework contract including the general terms and conditions of the contract not negotiated separately.

4. Neither the civil law, nor the sectoral legislation applicable to payment services – also including the EU legal acts serving as a basis for Hungarian sectoral legislation – provide an itemised list for conduct qualifying as gross negligence. However, it can be established based on Recital 72 of PSD2[3] and the higher court practice that differentiation should be made between simple fault and negligence and gross negligence. Gross negligence usually manifests itself in strikingly irrational and unreasonable infringement, close to wilfulness. Due to the foregoing, the MNB expects payment service providers to specify, as a norm, in the information and framework agreement, only such conduct as gross negligence, – close to wilfulness – that is more severe than a simple fault or negligence. The MNB reminds payment service providers to take into consideration the case-law of Hungarian courts, in addition to the provisions hereof, when assessing the actions of the customer.[4]

5. Furthermore, the MNB reminds payment service providers that with a view to keeping the payment instruments and the personal authentication data necessary for the use of those safe, the rules of

---

[1] Article 43 (2) of the Payment Services Act provides that "In the case of a request for rectification in connection with an unauthorised payment transaction – including, where appropriate, the payment initiation service provider –, the use of a payment instrument alone shall not necessarily be sufficient to prove either that the customer acted fraudulently or that they authorised the payment transaction or breached their obligations under Article 40 (1) and (2) deliberately or with gross negligence".

Pursuant to Article 40(1) of the Payment Services Act cited above, the customer or the entity authorised to dispose over the customer's payment account must use the payment instrument as it is specified in the framework contract, and in order to keep the payment instrument and the personal authentication data, necessary for its use, secure, they must adopt a conduct expectable in the given situation. Furthermore, pursuant to Article 40(2) of the Payment Services Act, the customer or the entity authorised to dispose over the customer's payment account shall immediately notify the payment service provider or any third person designated by it of any case when he perceives that the payment instrument is no longer in the customer's possession, or it has been stolen, or is used by an unauthorised person or without authorisation.

[2] Pursuant to Article 45(3) of the Payment Services Act, the payment service provider shall be exempted from the liability under Article 45(1), (2) and (4) of the Payment Services Act, if it proves that the loss incurred in connection with the unauthorised payment transaction was caused by the payer acting fraudulently or by breaching his obligations under Article 40(1) and (2) of the Payment Services Act intentionally or through gross negligence, particularly if they transfer or disclose their personal authentication data necessary for the use of payment instruments to an unauthorised third party.

[3] According to Recital 72 of PSD2 "In order to assess possible negligence or gross negligence on the part of the payment service user, account should be taken of all of the circumstances. The evidence and degree of alleged negligence should generally be evaluated according to national law. However, while the concept of negligence implies a breach of a duty of care, gross negligence should mean more than mere negligence, involving conduct exhibiting a significant degree of carelessness; for example, keeping the credentials used to authorise a payment transaction beside the payment instrument in a format that is open and easily detectable by third parties. […]".

[4] See, for example, the decision of the Budapest Court of Appeal No Pf. 20.055/2020/5, Pf. 20.259/2020/5 or Pf. 20.020/2021/5.

conduct, constituting the customers' contractual obligation, may be specified in the information and in the framework contract, but of those contractual obligations they may specify only those as a typical case of the customer's wilful conduct or gross negligence that represent more severe infringement than generally expected, going beyond the degree of negligence. In addition to the foregoing, the MNB also reminds payment service providers that the customer's request for rectification must be investigated case-by-case, considering all details of the incident, even in a typical case of the customer's wilful conduct or gross negligence as specified in the framework contract.

IV. Expectations with regard to the delivery of new payment instrument to the customers

6. The MNB expects the payment service provider to notify the customer without undue delay, in the form of communication through electronic channels, on the activation of the new, card-based payment instrument (e.g. payment card or credit card, including the renewal of these instruments due to expiry), after which date the customer may start the use of the cash substitute instrument, with restrictions, where applicable. The MNB expects the payment service provider to charge no fee, cost or other payment obligation for such notification, and to ensure that the notification includes – among others – the clear designation of the cash substitute instrument and that by using the respective payment instrument, payment orders may be initiated and approved.
7. If the payment service provider provides the customer with a new, non-card based payment instrument, such as a mobile or internet banking application – including also the reinstallation of the application – the MNB expects the payment service provider to notify the customer without delay through an electronic channel. Furthermore, the MNB expects the payment service provider to send the notification hereunder to the customer not through the newly provided payment instrument, i.e. the information should not be provided e.g. within the newly installed mobile application, but it should rather apply a solution for communication through a different electronic channel.
8. In the course of applying electronically for or registering a new, non-card payment instrument, and at the time of its first use, e.g. logging into the application for the first time – particularly when the payment instrument is registered under a device or telephone number not used previously by the customer – the MNB expects the payment service provider to apply tighter security measures than its general practice. Accordingly, the MNB expects the payment service provider to send the customer an additional confirmation message following the application for, registration and first use of the new non-card payment instrument in the form of communication through an electronic channel other than this payment instrument, and not to apply exemption from strong customer authentication.
9. The MNB expects the payment service provider to include in the notifications specified in points 6 and 7 a clear warning that the reason for sending the notification is the application for, registration or first use of the new payment instrument, and the notification should also include information on how the customer can immediately notify the payment service provider if the application, registration or first use was initiated not by them.

V. Expectations with regard to the development of lines of defence preventing external and internal frauds

10. The MNB regards it as good practice if payment service providers make efforts, in line with the relevant laws and the directly applicable EU legal acts,[5] to share with each other any information implying abuses as soon as possible, and to cooperate with other institutions, such as the authorities or the financial enterprise operating the payment system, for the purposes of preventing and identifying abuses and mitigating the losses.

11. As part of compliance with Article 41(3)[6] of the Payment Services Act the MNB expects payment service providers to provide customers with solutions, in particular electronic communication facilities (including robot-controlled recorded telephone solutions), where customers can report abuse without waiting and then, if justified, to comply with the obligation under Article 45(4)[7] of the Payment Services Act, after having received the information necessary for taking the appropriate measures. The MNB also expects payment service providers to put in place mechanisms to cancel suspected fraudulent orders as soon as possible after the customer has reported the fraud and to start recovering the amount of the fraudulent payment transaction.

12. The MNB expects the payment service provider to use cross-identification or at least an equivalent method in terms of security when authenticating the customer over the telephone or other voice-based means that do not require the personal presence of the customer and facilitate direct communication, in respect of questions of authentication nature concerning the customer's personal data.

13. The MNB regards it as good practice for payment service providers to allow their customers to specify a unique identification code for the use of electronic channels, which the payment service provider must use to identify itself to the customer in the course of communications through electronic channels initiated by the payment service provider (for example, in the case of a telephone call from the payment service provider's customer service).

14. The MNB regards it as good practice if payment service providers provide customers with the possibility to block the sender of a payment request that they consider to be suspected of abuse and to unblock the payment request without the intervention of the payment service provider's representative, through electronic communication, such as using a mobile or internet banking application.

15. The MNB expects that the investigation of abuse should also cover aspects of possible involvement of the payment service provider's employees (retroactively for a period commensurate with the risks) with appropriate continuous safeguards, and, where internal involvement is proven, in particular direct (e.g.

[5] For example, the provisions of Article 45 of Regulation 2022/2554/EU of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations No 1060/2009/EC, No 648/2012/EU, No 600/2014/EU, No 909/2014/EU and 2016/1011/EU (DORA), applicable from 17 January 2025.

[6] Pursuant to Article 41(3) of the Payment Services Act, the payment service provider shall make sure that the customer can make the respective notification specified in Article 40 (2) of the Payment Services Act, or request the termination of the blocking specified in Article 39 of the Payment Services Act, free of any fee, charge or other payment obligation.

[7] Pursuant to Article 45(4) of the Payment Services Act, after the notification made under Article 40(2), the payment service provider shall bear all losses relating to any unauthorised payment transactions resulting from the use of a lost or stolen payment instrument, or from the unauthorised use of a payment instrument.

by customer service, branch representative) or indirect (e.g. by IT staff) access to the payment account affected by the abuse, the modification of static data related to communication.

VI. Considerations applicable to the planning and application of the IT environment and process controls[8]

16. With a view to preventing abuse, the MNB expects payment service providers to take at least the following measures

    a) to define and apply logging requirements for all system components (e.g., application, application server, database, operating system, network security devices) involved in each payment service or other related service to ensure the recording of events necessary for investigating abuses[9],

    b) the logging of payment transactions in the IT systems is designed in such a way that it is capable of reconstructing the entire process in the event of a potential abuse, it includes the payment account details in the case of the use of a secondary account identifier and, in the case of a payment order given by means of a payment instrument, the parameters of the payment instrument and the available parameters of the IT tool required for its use, and the fact that confirmation codes or messages have been sent in relation to the payment transaction, keeps a strict, time series-based log of the payment transactions where the time sequence can be accurately verified, including by comparison with other payment transactions, and should not allow the subsequent modification of completed payment transactions, unless such a modification is logged in accordance with the payment service provider's payment transaction modification procedures, in particular authorised by the competent manager in a logged manner,

    c) to log events related to payment transactions.

17. In order to ensure the security of the customer's data, assets and instruments, the MNB expects the payment service provider to ensure at least the following:

    a) in the case of all transactions carried out by the customer in the payment service provider's system which relate to the customer's personal data, data classified as financial sector secrets (for example, banking secret under the Credit Institutions Act or payment secret under the Payment Service Provider Act) or their assets or property managed by the payment service provider, the customer's identity and the transaction carried out can be clearly identified,

    b) based on the customer's prior request, the payment service provider shall immediately notify the customer, by electronic communication, of updates in the balance of the payment accounts as specified by the customer, in his personal authentication and notification data (hereinafter

[8] Pursuant to Article 4(2) of the Decree, the software must be collectively suitable for recording the data necessary to operations and prescribed by law, for keeping secure records of funds and financial instruments, for connecting directly or indirectly to national IT systems related to the institution's activities, including the reporting of payment accounts to the Company Court, for using the stored data for verification purposes, and for providing logical protection commensurate with the security risk and for protecting integrity.

[9] For example, in the case of an abuse, the activities of the customer or intruder involved in the abuse and the related information.

collectively: transaction monitoring message),

c) when sending a transaction monitoring message to the customer, the payment service provider must ensure that it is clear to the customer exactly what he is informed of and exactly what transaction (e.g. a payment order) is in the process of execution, for what amount and toward which beneficiary (based on the information received from the receiving service provider),

d) the payment service provider should provide its customers qualifying as consumers and micro-enterprises with the possibility of immediate transaction monitoring related to payment accounts, payment instruments and changes to personal identification and notification data – free of charge, costs or other payment obligations – unless the customer has expressly waived this possibility of monitoring,

e) where the payment service provider transfers personal data or financial sector secrets to the customer by means of a non-secure communication solution (e.g. an e-mail notification), it should encrypt the notification prior to transmission and provide the customer with the application or instructions necessary to decrypt the notification (e.g. information on password protection and how to generate the generated password) and the key, by using a different communication solution prior to sending the notification,

f) the payment service provider should ensure the non-repudiation of the message having been sent by means of a client-side electronic signature and a time stamp for messages related to payment transactions, or the existence of the messages at a given moment of time by means of a server-side electronic signature and a time stamp for messages generated at the time of their receipt or transmission,

g) the payment service provider should authenticate and ensure the safekeeping of messages relating to payment transactions and ensure their retrievability and verifiability for the period prescribed by the applicable laws.

18. The MNB regards it as good practice for the security of the customer's data, assets and funds if the payment service provider ensures that

a) push messages sent to the customer from the mobile application, which may as well be readable on a locked screen, do not contain sensitive payment data[10] by default, they are made accessible only after authentication instead;

b) sensitive payment data within the mobile application should not be accessible from outside the mobile application (for example, by blocking out areas containing sensitive payment data to protect against screen mirroring).

19. The MNB expects payment service providers to pay particular attention to the prevention of abuses, such as phishing attacks or attempts at deception, especially when introducing a new IT system, replacing an existing system, or performing significant changes to it, irrespective of whether these are

[10] Pursuant to point 5a of Article 2 the Payment Services Act, sensitive payment data are data that can be used for committing fraud, including personal authentication data, with the proviso that the name of the account holder and his payment account number are not sensitive payment data for the purpose of the payment initiation service or account information service.

related to changes in legislation or business needs.

20. The MNB expects payment service providers to develop and implement procedures for monitoring and blocking phishing websites affecting their services and for informing customers about phishing campaigns.

VII. Expectations with regard to fraud analyses

21. The MNB expects the payment service provider to monitor prevailing abuse trends and fraud scenarios; in addition to professional sources, to analyse abuses affecting its own customers at regular intervals, and to analyse how the abuse could have been avoided. The MNB also expects the payment service provider to incorporate the results into its monitoring and prevention processes and to prepare an action plan to reduce the number of abuses.

22. The MNB expects payment service providers to take the prevention of abuse into consideration as early as in the design and product development phase when introducing a new payment instrument or authentication procedure, and when introducing, replacing or significantly modifying a new IT system affecting payment transactions. The MNB also expects the payment service provider to monitor any abuses and vulnerabilities related to the introduction of a new product or IT system for a period of time commensurate with the risks, the complexity and volume of the change, in addition to the usual procedures of the payment service provider, and to ensure that any identified deficiencies and vulnerabilities are promptly remedied.

VIII. Expectations with regard to improving customers' security awareness

23. With regard to the framework of risk mitigation measures and control mechanisms established pursuant to Article 55/A(1)[11] of the Payment Services Act, the MNB expects the payment service provider

    a) to have a customer education strategy to increase overall security awareness in line with the payment habits of its customers,
    b) to define measures in the customer education strategy, including recurring measures that foster the enhancement of its customers' security awareness – in relation to the financial and supplementary financial services provided by the payment service provider – in order to prevent abuses affecting customers to the highest possible degree.

24. As regards the customer education measures to be applied, the MNB expects payment service providers to provide their customers with simple and clear information or messages related to current or pending risks regularly, at a prominent place and in a manner suitable for raising customer's awareness of the risks of abuse. As regards the definition of a prominent place and manner suitable for raising attention, the MNB regards it as good practice to differentiate by customer groups, taking into consideration the typical patterns of using payment services by individual customer groups.

[11] Article 55/A(1) of the Payment Services Act provides – among other – that payment service providers shall establish a framework of risk mitigation measures and control mechanisms to manage operational and security risks related to the payment service provided by them.

25. The MNB expects the payment service provider to present the known risk elements and patterns of abuse and the ways to avoid them in a clear and understandable manner, using graphic practical examples, as part of the information provided under point 24.

26. The MNB expects the messages to inform customers under points 24 and 25 should not be overgeneralised and not to contain long descriptive texts or foreign words. Accordingly, the MNB expects payment service providers to avoid paper-based letters or e-mails containing long and difficult to understand financial, payment or IT industry jargon, as well as regular push messages and short text messages (SMS messages), which are less likely to attract attention and may result in customers perceiving them as unsolicited messages, which therefore they disregard or delete.

27. The MNB regards it as good practice for payment service providers to use attention-grabbing infographic solutions and short animated videos for the purposes of customer information in the mobile and internet banking applications and on the welcome screens of those as well as in the interfaces related to the initiation of payment orders. The MNB regards it as good practice to provide attention-grabbing information in the form of push messages and short text messages (SMS), which – considering the provisions of point 26 – briefly and clearly draw attention to a specific abuse or the risk of abuse in relation to a specific fraud case or pattern rather than repeating a long text message on a regular basis.

28. The MNB expects payment service providers to ensure that the form and content of messages sent to customers do not carry the features of unsolicited messages, and thus the links in the message should point to the payment service provider's website; if the message is sent to the customer by e-mail, it should come from the payment service provider's domain, and the payment service provider should not use marketing elements, and the tone of the message should not be urging or demanding.

29. In addition to the general information, the MNB regards it as good practice for payment service providers to use a warning message proportionate to the risk of the specific payment transaction, for example as part of the authentication process carried out by the payment service provider, when the customer uses payment services – especially when initiating a payment or submitting a payment order – in order to prevent payment orders that are presumably against the customer's intentions. When assessing the riskiness of payment transactions, the MNB regards it as good practice for payment service providers to take into consideration the risk level determined as a result of the transaction monitoring mechanisms operated based on Article 2 of the SCA Regulation[12]. The MNB regards it as good practice for the payment service provider in the case of a payment transaction of higher risk value to draw the customer's attention to the potential risks and to the need to double-check the payment details – such

[12] Pursuant to Article 2(1) of the SCA Regulation, payment service providers shall have in place transaction monitoring mechanisms that enable them to detect unauthorised or fraudulent payment transactions for the purposes of implementing the security measures referred to in Article 1(a) and (b) of the SCA Regulation. Those mechanisms should be based on the analysis of payment transactions, taking into account elements that are specific to the payment service user under the circumstances of normal use of personal authentication data.

Article 2(2) of the SCA Regulation provides that payment service providers shall ensure that the transaction monitoring mechanisms take into account at least each of the following risk-based factors:

a) list of no longer secure or stolen authentication elements;
b) amount of the individual payment transactions;
c) known fraud scenarios in the provision of payment services;
d) signs of the presence of malware in any session of the authentication procedure;
e) where the access device or software is provided by the payment service provider, the log of the use of the access device or software provided to the payment service user and the abnormal use of the access device or software.

as a new beneficiary, an amount that is unusually high compared to previous payment habits, or significantly different consumer behaviour (e.g. unusual way of initiating a payment, the currency, geographical location, time, method and means of accessing the payment instrument of the payment order given, with the use of a different payment instrument from the one previously used to submit payment orders) or elements similar to known trends of abuse or fraud scenarios in the provision of payment services.

30. The MNB expects payment service providers to pay special attention to raising customers' security awareness in relation to the introduction of new IT systems for payment transactions, the replacement of existing IT systems, significant changes to these IT systems or fraud opportunities related to changes in legislation. In particular, the MNB expects payment service providers to warn customers of possible phishing attacks or attempts to mislead in connection with the implementation of the IT system.

31. The MNB expects the payment service providers that when raising customer awareness they should draw customers' attention to

    a) the possibility of instant transactions monitoring – provided free of charge in accordance with the MNB's requirements – especially to the possibility of monitoring payment accounts and payment instruments, provided by the payment service provider through electronic communication channels, in particular in the form of push messages or short text messages (SMS), for security purposes, and their importance in detecting and preventing abuse,

    b) how the customer can fulfil the notification obligation required by Article 40(2) of the Payment Services Act and how to report abuse to the police,

    c) the transaction threshold amounts and the options to modify the thresholds applicable in certain services to protect the assets of customers,

    d) solutions available from the payment service provider to manage customers' assets more securely, such as the virtual payment cards, which can be used for transferring only the amount of money justified, e.g. by payment habits or needed for a one-time payment transaction, thereby reducing the possibility of fraud and potential losses.

32. The MNB regards it as good practice for payment service providers issuing card-based payment instruments to remind cardholder customers regularly to save their payment card data only on trusted payee platforms and primarily only for recurring transactions (e.g. utility bill payments).

33. With a view to increasing customers' security awareness, the MNB expects payment service providers to pay special attention to the training of customer service representatives to prevent incomplete or incorrect information being provided to customers.

34. The MNB expects payment service providers to provide regular training for customer service representatives on how to recognise fraud attempts and prevent phishing and, where appropriate, data leakage.

35. The MNB regards it as good practice for payment service providers to take the European Commission's Financial Awareness Framework[13] and the financial literacy framework for adults[14] into account when implementing measures to enhance customers' security awareness.

IX. Expectations with regard to transaction limits and restrictions connected to payment transactions

36. The MNB expects payment service providers to define and apply transaction limits for each payment instrument issued by them, in particular mobile banking, internet banking and payment cards. The MNB expects the defined transaction limit to be aligned with the payment habits of the payer or a group of payers, both in terms of value and number of items, and to simultaneously prevent the execution of unusual payment transactions. The MNB expects the payment service provider to provide the holder of a payment instrument with the option to change the transaction limit up to a ceiling set for a group of payers based on their payment habits, different for each payment instrument where applicable, upon the request of the holder of the payment account. The MNB reminds payment service providers that pursuant to Article 55/C(1)c)[15] of the Payment Services Act, the transaction limit may only be changed after strong customer authentication. The MNB also expects that, in the case of reducing the previously set transaction limit, the change should be possible not only for a temporary period. The MNB expects payment service providers to provide their customers with the option to change transaction limits free of charge by means of electronic communication (e.g. via an internet banking or mobile banking application) without the cooperation of the payment service provider's representative.
37. The MNB regards it as good practice for a payment service provider to set the transaction limit for a specific payment instrument at a level significantly lower than the one specified in point 36 for a period of 24 hours after the activation of the payment instrument, which prevents high-value frauds while it does not prevent the customer from making his normal daily payments based on his previous payment habits. In addition, the MNB regards it as good practice for the payment service provider not to allow the customer to increase the transaction limit for the respective payment instrument within this period through a remote communication channel.
38. The MNB regards it as good practice for payment service providers to strive for simplicity and to ensure that the amendment can be made easily when lowering the transaction limit.
39. The MNB regards it as good practice for payment service providers to provide the option of setting a validity period and also an indefinite period when changing the transaction limit.
40. The MNB expects payment service providers to stipulate in its procedures the methodology for determining and establishing transaction limits as well as other aspects taken into consideration during the development of the methodology. The MNB expects payment service providers upon reviewing those regulations to give due consideration to the experience gained in dealing with abuses that have

[13] https://ec.europa.eu/info/business-economy-euro/growth-and-investment/capital-markets-union/capital-markets-union-2020-action-plan/action-7-empowering-citizens-through-financial-literacy_en
[14] https://finance.ec.europa.eu/publications/commission-and-oecd-infe-publish-joint-framework-adults-improve-individuals-financial-skills
[15] Pursuant to Section 55/C(1)(c) of the Payment Services Act, a payment service provider shall apply strong customer authentication when the payer carries out any action through a remote channel which may imply a risk of payment fraud or other abuses.' carries out any action through a remote channel which may imply a risk of payment fraud or other abuses.

occurred in the period since the previous review, i.e., the role of the applied limits in the prevention of abuses in the respective period.

41. The MNB draws attention to the fact that payment service providers inform their customers about the options to change the transaction amount limit for various payment instruments when providing information before concluding the framework contract in accordance with Article 10(1)b)bf) of the Payment Services Act.

42. If the increase of the transaction limit is initiated by the customer through a solution that allows direct communication, including voice transmission (e.g. over the phone or through a video banking solution), the MNB expects the payment service provider's representative to ask additional questions of authentication nature in addition to the authentication used by the payment service provider, if the authentication used before increasing the transaction limit did not cover these. The MNB expects the payment service providers to ensure that these questions:

    a) relate to the payment habits of the customer, his relationship with the payment service provider and the answers to these questions are known only to the customer concerned, and

    b) relate to the personal data of the customer,

    in respect of which the payment service provider applies the cross-identification method.

    The MNB draws attention to the fact that pursuant to Article 14(1)g) of the Payment Services Act, the payment service provider must specify the procedure applicable to transaction limits in the framework contract, such as the consequences of unsuccessful identification.

43. Furthermore, the MNB expects the payment service provider to refuse to modify the transaction limit if the answer to the questions specified in point 42 is incorrect and to record the fact of refusal in such a way that, in the event of a further transaction limit modification, it is clear to the payment service provider's current representative that the customer has already unsuccessfully attempted to modify the transaction limit before.

44. The MNB regards it as good practice for payment service providers to introduce a time limit (e.g. 24 hours) on the increase of the transaction limit initiated by communication via the respective electronic channel after the second failed attempt to increase the transaction limit, and to investigate the circumstances of the case within this time limit before lifting the restriction, preferably through contacting the customer.

45. When changing the transaction value limit, the MNB considers it good practice for the payment service provider's acting representative to ask questions about the reason for the change of the transaction amount limit and, if the response implies a potential abuse, to inform the customer without delay – through an electronic channel other than the one used to change the transaction amount limit, in particular by e-mail, push message or short text message (SMS) – of the potential risks associated with the increase of the transaction limit and the ways to obtain detailed information and further clarification from the payment service provider.

46. The MNB expects payment service providers to provide their customers with the option to stipulate in the framework payment contract that certain payment instruments – in particular mobile banking, internet banking applications or virtual payment cards – may only be used, at the customer's request, in the personal presence of the customer or through concluding or amending a framework contract using an audited electronic communication medium, as specified in MNB Decree No 26/2020 (VIII. 25)

on the detailed rules concerning the implementation of the Act on the Prevention and Combating of Money Laundering and Terrorist Financing, as applicable to service providers supervised by the MNB, and concerning the minimum requirements for the development and operation of the screening system under the Act on the Implementation of Restrictive Measures Imposed by the European Union and the UN Security Council Relating to Liquid Assets and Other Financial Interests (hereinafter: MNB Decree No 26/2020 (VIII. 25.).]. Namely, payment service providers are expected to provide the customer with the option to exclude the possibility of amending the contract electronically – with the exception of the audited electronic communication device under MNB Decree No 26/2020 (VIII. 25.) – for specific payment instruments (e.g. mobile banking or internet banking application), not including the amendment of the framework contract for the termination of the use of the payment instrument.

47. The MNB regards it as good practice for payment service providers not to allow the beneficiary to store or manage the payment card data of customers when accepting a card-based payment instrument, but to store or manage the payment card data that customers wish to store in the payment service provider's own IT solution or to provide the beneficiary with the possibility of doing so only by means of a tokenised solution or a solution offering at least equivalent security.

X. Expectations for the acceptance of strong customer authentication by third party service providers

48. If the payment service provider servicing the customer's payment account concludes an agreement not qualifying as outsourcing as specified in the Credit Institutions Act or in the Payment Service Provider Act to perform strong customer authentication in its own name with a payment initiation service provider, an account information service provider, or payment service provider issuing card-based payment instrument – not including electronic money – (hereinafter collectively: third party service provider), based on which agreement the strong customer authentication prescribed in Article 55/C(1) of the Payment Services Act[16] is executed the third party provider and not by the payment service provider servicing the customer's payment account, the MNB expects the payment service provider servicing the customer's payment account that prior to accepting the strong customer authentication by the third party service provider – and thereafter regularly, at least annually –, upon the modification of the third party service provider's strong customer authentication solutions, it should ascertain through an independent audit that the procedure applied by the third party service provider for strong customer authentication complies with the provisions of the Payment Services Act and the SCA Regulation as well as with the customer due diligence requirements of the AML Act.

XI. Expectations with regard to the mitigation of the risks attached to the multifunctional instrument providing any element of strong customer authentication

[16] Section 55/C(1) of the Payment Services Act stipulates that the payment service provider shall apply strong customer authentication when the payer accesses their payment account online, initiates an electronic payment transaction or carries out any action through a remote channel which may imply a risk of payment fraud or other abuses.

49. The MNB regards it as good practice for payment service providers to remind customers, primarily by electronic communication, to update regularly and apply available security patches to the multifunctional devices used by the customer and to use at least the following security settings:

    a) encryption of the data stored on the device,

    b) automatic locking of the screen of the device,

    c) using a PIN code of minimum 5 digits or other solution safer than that for unlocking the screen,

    d) installation of protection against malware (antivirus),

    e) creating regular backups.

50. The MNB expects payment service providers to investigate the signs of compromised integrity of multifunctional devices to a degree and with a frequency proportionate to the risks (e.g. more thoroughly when a new mobile application is used for the first time).

51. The MNB regards it as good practice for payment service providers to use the integrity validation solution provided by the vendor of the operating system to verify the integrity of multifunctional devices, if such a vendor solution is available.

52. On the basis of Article 4(2)(c) of the SCA Regulation and for the purposes of Articles 6–8 of the SCA Regulation, the MNB expects payment service providers to apply limits to payment or other payment-related transactions that can be executed by multifunctional devices of compromised integrity (e.g. hacked – (rooted or jail-broken) in proportion to the risks involved.

53. The MNB regards it as good practice for payment service providers not to allow the use of multifunctional devices of compromised integrity (e.g. hacked – rooted, jail-broken). In addition, the MNB regards it as good practice for payment service providers to carry out a preliminary risk assessment of the reliability of the operating system of the multifunctional devices used by their customers, and if the operating system of the multifunctional device used by the customer is not considered reliable based on the risk levels identified in the risk assessment (e.g. due to solutions used for scanning of elements qualifying as biological property by obsolete devices and operating systems which are easy to circumvent), the payment service provider should limit the execution of strong customer authentication, in particular when initiating a payment or issuing a payment order, depending on the risk level of the device concerned.

54. The MNB regards it as good practice for payment service providers to take into consideration the risk factors mentioned in Article 18(3) of the SCA Regulation when determining the extent of the limitation under point 53.

XII. Expectations with regard to transaction monitoring mechanisms related to frauds

55. For the purposes of Article 55/A(1) of the Payment Services Act and Article 2(1) of the SCA Regulation, the MNB expects the payment service provider to use an integrated transaction monitoring mechanism that analyses the risks associated with payment transactions, in particular the risks associated with users, activities and instruments, in a complex manner and in real time, for all payment methods related to the payment account as defined in the Payment Services Act. The MNB also expects payment service providers to perform the aforementioned real-time analyses in cases where there is an obligation for strong customer authentication for the payment transaction pursuant to Article 55/C(1)b) of the

Payment Services Act, and also when the payment service provider uses any of the exceptions specified in Chapter III of the SCA Regulation, and when the payment order is given on paper or over the phone.

56. As regards the development of the transaction monitoring mechanism under point 55, the MNB regards it good practice if the solution used by the payment service provider incorporates all technologies available to the payment service provider, in particular rules-based abuse prevention monitoring systems as well as artificial intelligence-based solutions, machine learning algorithms – including supervised and unsupervised machine learning solutions or e.g. clustering techniques – which are suitable for customer profiling.

57. The MNB expects payment service providers to assign a risk value to the respective payment transaction in connection with the transaction monitoring mechanisms under Article 2(1) of the SCA Regulation, designed in the light of the requirements set out in Article 2(2) of the SCA Regulation and in this Recommendation. The payment service provider may dispense with the definition of the risk value when implementing this point if it has an equivalent alternative solution which ensures the implementation of the measures it has developed in line with point 58.

58. Pursuant to Article 55/A(1) of the Payment Services Act the payment service provider must have a framework of risk mitigation measures and control mechanisms in place in order to manage operational and security risk. In connection with this, the MNB expects payment service providers to prepare procedures as part of the framework, where they define risk levels and assign measures to each risk level. Such measures may include, in particular, the suspension or refusal of the execution of the payment transaction, contacting the customer, waiving the application of the exception rule for strong customer authentication mentioned in Chapter III of the SCA Regulation, or contacting the competent criminal investigation authority. The MNB expects the payment service provider to take the measures specified in the procedures under this point without delay in relation to the payment transactions of a specific risk value, giving due consideration to the special features of the execution of the payment transaction concerned, in particular the execution deadlines prescribed in the MNB Decree.

59. The MNB expects the payment service provider to perform regular documented validation and evaluation of the efficiency of the transaction monitoring mechanisms in accordance with Article 3 of the SCA Regulation.

60. The MNB expects payment service providers to take into consideration the following risk-based factors in addition to those specified in Article 2(2) of the SCA Regulation:

    a) when it receives an unusually large number of payment orders to the debit or credit of a payment account (e.g., an unusually large number of instant payments in the case of the respective payment account); and

    b) a notification from any natural person which gives rise to a reasonable suspicion of abuse.

61. The MNB regards it as good practice if the payment service provider designs its transaction monitoring mechanism in such a way that it takes into consideration the relationship between different risks and risk-based factors (e.g., a joint assessment of a suspected fraudulent transfer following the registration of a new mobile application has already been classified as risky).

62. The MNB expects payment service providers to take into consideration at least the following risk-based factors when applying Article 2(2)(c-e) of the SCA Regulation:

a) the customer installing a new payment instrument (e.g., mobile banking application) on a device unknown to the payment service provider,

b) the use of IT tools and IP addresses used in previous abuses and known to the payment service provider,

c) known fraud scenarios based on misleading the customers, details of known frauds (e.g., payment accounts known to have been affected by the fraud, payment account that the amount of payment transactions was credited to, secondary account identifiers, countries involved, other parameters of payment transactions),

d) location and network (e.g. VPN, proxy usage) data of the device or software used for access,

e) use of the access device in a different way than before, such as typing speed or cursor movement, unusual language settings,

f) signs of the presence of malware in any phase of the authentication procedure.

63. The MNB regards it as good practice for payment service providers to take into consideration the following risk-based factors when applying Article 2(2)€-(e) of the SCA Regulation:

a) signs implying remote connection to the device or software used for access (e.g., screen mirroring),

b) parameters of the runtime environment of device or software used for access (e.g., emulator environment),

c) the number devices or software used for access (e.g., number of payment cards) does not match the customer's profile,

d) the payer and the beneficiary may have had a presumed business relationship (for example, a public utility company qualifying as reliable beneficiary),

e) payments made to the customer's own name.

64. The MNB expects the payment service provider to take into consideration at least the following factors with regard to the abnormal use of the access device or software under Article 2(2)e) of the SCA Regulation:

a) the amount, number and currency of the submitted payment orders, time and speed of submission, which may imply payment orders generated by an IT tool, location (e.g., blacklisted location or payment orders submitted in a short time from locations at a large distance from each other), compared with other customer groups with similar customer characteristics, in particular following the use of a new service not previously used by the customer, the assignment of a new secondary account identifier or the setting of a new transaction limit,

b) the aggregate value of the submitted payment orders, especially if it is approximately equal to the balance of the payment account,

c) payment orders close to the applied transaction limits,

d) of the submitted payment orders, payment orders initiated by the payer in respect of a beneficiary for whom no payment has been made earlier, in particular where the amount, number of items, currency or timing (e.g. time of day, frequency) of the payment transactions is unusual compared to categories of other customers with similar customer characteristics,

e) unusually high number of reversals concerning the payment account,

f) based on the patterns associated with a payment transaction to the debit or credit of a payment account, the payment account is likely to be involved in a transfer chain (known as mule account), e.g. by means of atomisation or cash-out, including the purchase of crypto-assets,

g) cash withdrawals debited to a payment account, including foreign currency withdrawals, regardless of whether the withdrawal is made in Hungary or in another country.

65. The MNB expects the payment service provider to apply the transaction monitoring mechanisms under Article 2 of the SCA Regulation to transactions relating to data entry solutions under point 1 of Article 2(1), single data entry solutions under point 4a of Article 2(1), requests to pay under point 5 of Article 2(1), and secondary account identifiers under point 12 of Article 2(1) of the MNB Decree, especially when

a) a secondary account identifier is assigned to the payment account suitable for deception,

b) the value or number of requests to pay or the timing of their submission is different from the submission patterns of customers with similar customer characteristics,

c) requests to pay are initiated from the payment account at an unusual time for particularly high amounts or in particularly large number,

d) a request to pay initiated from the payment account to a new addressee for an unusually high amount or in a particularly large volume in a short period,

e) the payment account receives a request to pay from a new beneficiary, at an unusual time, referring to an unusual payment situation or for a particularly large amount.

66. The MNB expects that during the use of transaction monitoring mechanisms under Article 2 of the SCA Regulation the payment service provider should take into consideration its (screening) system supporting the fulfilment of the notification defined in Article 63(1)b) of the AML Act and adjust its solutions to the existing screenings.

67. If the tasks related to the transaction monitoring mechanisms under Article 2 of the SCA Regulation and to the (screening) internal control and information system supporting the fulfilment of the notification under Article 63(1)b) of the AML Act, – including also the management of the alerts generated by the IT systems are carried out by the employees of functional areas operating in different organisational units, the MNB expects these functional areas to coordinate their activity and act jointly with a view to preventing frauds and money laundering.

XIII. Expectations with regard to the requests for rectification related to unauthorised payment transactions

68. Pursuant to Article 44(1) of the Payment Services Act, in the case of executing an unauthorised payment transaction – irrespective of whether it was initiated through a payment service provider rendering payment initiation services or not, the payment service provider servicing the payment account of the payer – unless in the respective situation it suspects a fraud on reasonable grounds, and informs the MNB in the report MNB identification code P65 of this – shall, immediately after obtaining knowledge or having been informed of the transaction, but no later than by the end of the next working day, reimburse the payer for the amount of the unauthorised payment transaction and reinstate the

payment account to the status before the debit entry, with the proviso that the value date of the credit entry shall not be later than the date of the execution of the unauthorised payment transaction.

69. The MNB reminds the payment service providers that, although EU directives – unlike EU regulations – are not directly applicable in the Member States, the standard text and preamble of the directives provide guidance for the correct interpretation of domestic legislation when interpreting the provisions of the directives transposing them into domestic law. In view of the foregoing, since Recital 71 of PSD2 provides guidance for the interpretation of Article 73(1) of PSD2, in the MNB's view the provisions of that Recital should be regarded as a guiding principle also for the interpretation of Article 44 of the Payment Services Act, for example, in respect of the deadline for investigation required by Government Decree No 435/2016 (XII. 16) on the detailed rules for the complaints handling procedure and the complaints handling regulations of investment firms, payment institutions, electronic money institutions, issuers of vouchers, financial institutions and independent financial service intermediaries (hereinafter: the Complaints Handling Decree). According to Recital 71 of PSD2, "where there is a high suspicion of an unauthorised transaction resulting from fraudulent behaviour by the payment service user and where that suspicion is based on objective grounds which are communicated to the relevant national authority, the payment service provider should be able to conduct, within a reasonable time, an investigation before refunding the payer."

70. The deadline of one working day mentioned in Article 44(1) of the Payment Services Act is calculated from the date of the customer's notification, but since according to the legislation Article 44(1) of the Payment Services Act only applies to the "*execution of an unauthorised payment transaction*", bearing this in mind, if the notification is made before the execution (debiting the payer's account), it is possible to wait until the date of the execution, but the required measures must be taken immediately thereafter, i.e. the deadline of "*but not later than by the end of the following working day* " no longer applies.

    Based on the foregoing, the MNB draws attention to the fact that the notification submitted through the report of MNB identification number P65 shall not exempt the payment service provider from its liability for damages. However, it shall be exempted from compliance with the one working day deadline for the reimbursement of the amount of the unauthorised payment transaction specified in Article 44(1)a) of the Payment Services Act. In the MNB's view, the purpose of the cited provision of the Payment Services Act is – in line with recital 71 of PSD2 – to allow the payment service provider to investigate the complaint properly, instead of exempting it from liability for damages temporarily. The purpose of informing the MNB is to ensure that the payment service provider servicing the customer's payment account reimburses the customer within one working day at the latest, unless it suspects fraud on reasonable grounds in the given situation due to reasons it has informed the MNB of. For this reason, the MNB expects payment service providers to make the notification to the MNB in report of MNB identification code P65 only if the payment service provider's suspicion of abuse is duly substantiated.

71. The MNB expects the payment service provider to examine the circumstances of the execution of each payment transaction that has not been authorised by the payer and is subject to a request for rectification on an individual basis, taking into account all details.

72. The MNB also draws attention to the fact that in order to keep the payment instrument and the personal identification data required for its use safe, the payment service provider specifies the rules of conduct – which constitute the contractual obligation of the customer – in the framework contract, but may, when judging a request for rectification in relation to the execution of an unauthorised payment

transaction, classify any conduct or omission breaching the rules of conduct laid down in the framework contract, leading to the occurrence of losses the possibility of losses resulting from the execution of the unauthorised payment transaction as intentional or grossly negligent conduct based on the revelation of other circumstances indicating the conduct of the customer concerned.

Therefore, for example, in the case of a fraud connected to cash withdrawal with the use of payment card, the fact that the fraud was committed by using the PIN code belonging to the payment card alone does not prove that the customer acted fraudulently, or breached their obligations under the Payment Services Act or the framework contract intentionally or through gross negligence, since the PIN code of the payment card can be obtained by other means, despite the customer acting with due care [e.g. by manipulating the automated representative machine (hereinafter: ATM)]. Due to the foregoing, the MNB expects payment service providers not to base the evidence under the Payment Services Act solely on the use of (strong) customer authentication data, as this is prohibited by Article 43(2) of the Payment Services Act, as the authentication during the use of the device forms part of using the payment instrument itself. However, the authentication data, together with other evidence (such as, in the example above, a recording from the ATM camera or, in other cases, a statement by the customer that they wrote the PIN on a piece of paper and kept it with the payment card), may evidence fraudulent, intentional or grossly negligent behaviour by the customer.

73. Pursuant to Article 43(2) of the Payment Services Act, considering that the short text message (SMS), push message or other information related to the authorisation of a payment transaction is part of the use of a payment instrument, the sending of such messages by the payment service provider alone shall not serve as evidence of fraudulent conduct or intentional or grossly negligent behaviour of the customer, and thus the payment service provider is expected to reveal other circumstances as well and use those as evidence.

74. The MNB expects the payment service provider that upon rejecting the payer's request for rectification:

    a) it should explain in detail the reasons for its position, the evidence it has gathered and the assessment of the evidence as well as the conclusions drawn from it,

    b) should not make assumptions or logical deductions based on assumptions about the customer's behaviour,

    c) in the evidence procedure it should take into consideration all relevant circumstances of the individual case and all relevant information available about the specific person who authorised the payment transaction.

75. The MNB draws attention to the fact that, in the case of responding to requests for rectification, if the payment service provider fails to notify the MNB within the framework of reports of MNB identification code P65, pursuant to Article 44(1), Article 43(2) and Article 45(3) of the Payment Services Act, the payment service provider shall have one working day to reimburse the amount of the payment transaction to the customer or to reject the request for rectification, stating the reasons on the basis of the relevant evidence, and, in the latter case, to send the customer a reply by the deadline prescribed in the Complaints Handling Regulation. The MNB also draws attention to the fact that if the payment service provider makes a notification to the MNB pursuant to Article 44(1) of the Payment Services Act in the report of MNB identification code P65, in accordance with this Recommendation, the payment service provider is also deemed to have acted within the deadline specified the Complaints Handling Regulation when responding to the request for rectification.

The MNB reminds payment service providers that the charge-back procedure used by international card companies does not exempt payment service providers from complying with the liability and procedural rules prescribed in the Payment Services Act, in particular with regard to the deadlines for restoring the payment account to its original state and the requirements applicable to evidence. The MNB also notes that the data and information that become available to the payment service provider as a result of a charge-back procedure may be used as evidence in the fulfilment of the burden of proof prescribed by the Payment Services Act.

In the absence of submitting the report of MNB identification code P65, the payment service provider shall be exempted from its refund obligation under Article 44(1) of the Payment Services Act, if it investigates the case in a verifiable manner within the deadline applicable to the credit entry under Article 44(1)a) of the Payment Services Act and proves, in accordance with Article 43(2) and Article 45(3), that the disputed payment transaction was authorised by the payer or that the loss generated by the unauthorised payment transaction was caused by the payer acting fraudulently or that the loss was caused by the payer through the wilful or gross negligent breach of his obligations specified in Article 40(1) and (2) of the Payment Services Act, in particular if, by their intentional or grossly negligent conduct, they provided or made available to an unauthorised third party the personal authentication data necessary for the use of the payment instrument. This is considered to be proven if the investigation includes an assessment of the circumstances, related data and information, and is documented in a form suitable for identifying the date of the finding.

76. The MNB reminds payment service providers that they must not oblige in any way the customer to report the case to the competent criminal investigation authority, but the MNB expects payment service providers to inform the customer that they should report the case to the competent criminal investigation authority and to provide assistance in making the report. Furthermore, the MNB expects the payment service provider not to treat the mere failure to make a report to the competent criminal investigation authority as grossly negligent behaviour, and not to define it as such in the framework contract either.

77. The MNB expects the payment service provider to comply with the reporting obligation prescribed in subtitle 11 of the AML Act, without delay, in writing, if any data, facts or circumstances imply that the property resulted from culpable offence.

XIV. Closing provisions

78. The recommendation is a regulatory instrument, issued in accordance with Article 13(2)i) of the Act CXXXIX of 2013 on the Magyar Nemzeti Bank, with no binding force on the supervised financial organisations. The content of the recommendation issued by the MNB expresses the statutory requirements, the principles proposed to be applied based on the MNB's law application practice as well as the methods, market standards and practices.

79. The MNB, in line with general European supervisory practice, monitors and assesses compliance with the recommendation during its audit and monitoring activity conducted at the payment service providers it supervises.

80. The MNB highlights that payment service providers may make the contents of this recommendation part of their policies. In such case, the payment service provider is entitled to indicate that the provisions of its relevant policies comply with the relevant recommendation issued by the MNB. If the

payment service provider wishes to incorporate only certain parts of the recommendation in its policies, it should not make reference to the recommendation as a whole or should only do so in respect of the parts taken from the recommendation.

81. The MNB expects the respective payment service providers to apply the recommendation – with the exception of the provisions of Articles 82 and 83 – from 1 January 2024.

82. The MNB expects the respective payment service providers to apply Articles 6–9, 13, 14, 17(d), 29, 36–41, 44–47 and 49–54 from 1 September 2024.

83. The MNB expects the respective payment service providers to apply Articles 55–67 from 1 March 2025.

Dr György Matolcsy
Governor of the Magyar Nemzeti Bank