Recommendation No 1/2020 (III. 4.) of the Magyar Nemzeti Bank

on the Procedures related to the payment service providers' handling of money transfers with incomplete data

I. Purpose and scope of the recommendation

The purpose of this recommendation is to formulate the expectations of the Magyar Nemzeti Bank (hereinafter: MNB) – and thereby to increase the predictability of the application of law and foster the uniform application of legislation – by determining the factors that the payment service providers and intermediary payment service providers (hereinafter: service providers) supervised by the MNB should take into consideration when elaborating procedures and execute measures related to money transfers the objective of which is to clarify missing or incomplete data related to the payer or the payee and to manage the fund transfers affected by such data.

The recommendation serves as a guide for the supervised service providers for the event when the necessary data related to the payer or the payee are not known to the service provider or they are incomplete. Furthermore, the recommendation intends to provide assistance to service providers in the efficient development of their activity concerning anti-money laundering and combating the financing of terrorism (hereinafter: AML/CFT), related to the aforementioned situations, in accordance with the requirements of risk-based approach.

The recommendation ensures compliance with Regulation 2015/847/EU of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation 1781/2006/EC (hereinafter: Regulation 2015/847/EU) and particularly with Articles 7–13 thereof.

When developing the recommendation, the MNB took into consideration the provisions of the Joint Guidelines JC/GL/2017/16 issued on 16 January 2018 by the European financial supervisory authorities, namely, by the European Banking Authority, the European Insurance and Occupational Pensions Authority and the European Securities Market Authority (hereinafter: ESA Guideline). Setting out from the requirements outlined in the ESA Guideline, the MNB defines in this recommendation the practice to be followed by the service providers.

The recommendation is addressed to payment service providers specified in point 5 of Article 3 of Regulation 2015/847/EU, with registered office or branch office in Hungary, having a business unit that offers payment services to customers in the form of actual domestic presence, acting as the payment service provider of the payee and to the intermediary payment service providers specified in point 6 of Article 3 of Regulation 2015/847/EU.

This recommendation shall not apply to the implementation of financial and property restrictive measures imposed by the UN Security Council or to restrictive measures imposed by regulations based on Article 215 of the Treaty on the Functioning of the European Union, including Regulation 2580/2001/EC, Regulation 881/2002/EC and Regulation 356/2010/EC.

The identification of the subjects of financial and property restrictive measures shall be carried out on the basis of other AML/CFT legislative provisions.

This recommendation does not fully refer back to the legal provisions when setting out the principles and expectations, but the addressees of this recommendation are of course still obliged to comply with the relevant legal requirements.

This 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. Definitions

For the purposes of this recommendation:

a) incomplete data: data relating to the payer or payee prescribed by Regulation 2015/847/EU, but provided only partially;

b) missing data: data relating to the payer or payee prescribed by Regulation 2015/847/EU but not provided;

c) risk: the occurrence or likelihood of money laundering and terrorist financing (hereinafter together: ML/TF). Risk shall mean the level of risk before risk mitigation (inherent risk) rather than the risk level after mitigation (residual risk);

d) risk-based approach: an approach whereby the MNB and the service providers identify, assess and interpret the ML/TF risks to which the service providers are exposed and enforce AML/CFT measures commensurate with such risks;

e) risk factors: variables that, alone or in combination with each other, may increase or decrease the ML/TF risk of a business relationship or transaction order;

f) subsequent monitoring: monitoring activity performed

i) after the funds have been credited to the payee's payment account by his payment service provider,

ii) if the payee has no payment account with his payment service provider, after the funds have been made available to the payee by the payment service provider receiving the transfer of funds or after the funds have been forwarded by the intermediary payment service provider; or

iii) in the case of an intermediary payment service provider, after the transfer of funds has been forwarded by the payer's payment service provider or by an intermediary payment service provider acting on behalf of another intermediary payment service provider

g) real-time monitoring: monitoring activity performed

i) before the funds are credited to the payee's payment account by his payment service provider,

ii) if the payee has no payment account with his payment service provider, before the funds are made available to the payee by the payment service provider receiving the transfer of funds, or

iii) in the case of an intermediary payment service provider, prior to the transfer of funds by the payer's payment service provider or by an intermediary payment service provider acting on behalf of another intermediary payment service provider

Unless provided otherwise, the terms used and defined in Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing (hereinafter: AML Act) and in Regulation 2015/847/EU shall have the same meaning in this recommendation as well.

III. Detection of missing data and management of transfers of funds sent with missing data

1. The MNB expects the service provider to apply written regulations and efficient procedures in order to comply with Regulation 2015/847/EU.

2. For each transfer of funds, the service provider shall determine whether it acts as the payment service provider of the payer or payee, or as an intermediary payment service provider. This determines the type of data that should accompany the respective transfer of funds and the steps that the service provider must take to comply with Regulation 2015/847/EU.

3. If the transfer of funds is a direct debit as defined in Article 3(9)(*b)* of Regulation 2015/847/EU, the payee's payment service provider shall send the prescribed information on the payer and the payee to the payer's payment service provider as part of the submission of the direct debit. In this case, the

payment service provider of the payee and the intermediary payment service provider may assume that the data disclosure requirements specified in Article 4(2) and (4) and Article 5(1) and (2) of Regulation 2015/847/EU are satisfied.

4. Compliance with Regulation 2015/847/EU by the service provider is required for all transfers of funds carried out at least in part by electronic means, regardless of the messaging or payment and settlement system used, unless Regulation 2015/847/EU provides for an exemption or possible derogation for the respective transfer of funds.

5. The service provider is expected to apply the exemptions and derogations provided in Regulation 2015/847/EU only if the conditions for their application have been established beyond reasonable doubt and in a provable manner prior to the execution of the transfer of funds.

6. When applying the exemption specified in Article 2(3) of Regulation 2015/847/EU, the service provider shall ensure that the number of the credit card, digital or other device, such as the primary account number (PAN), can be identified and recorded for the transfer of funds and that the number is provided in a way that allows the transfer of funds to be traced back to the payer.

7. The exemption specified in Article 2(3) of Regulation 2015/847/EU may be applied by the service provider only for transfers of funds where it is established beyond reasonable doubt that the transfer is not a person-to-person transfer of funds but rather it is for the purpose of payment for goods and services.

8. In order to apply the derogation specified in Article 5 of Regulation 2015/847/EU

a) the payee's payment service provider must be able to ascertain whether the payer's payment service provider is established in the European Union or in another state participating in the Agreement on the European Economic Area (hereinafter: EEA member state); and

b) the intermediary payment service provider must be able to ascertain whether the service providers in the payment chain are established in the European Union or in an EEA member state.

9. The country of the registered office, branch or business site of a payment service provider in the payment chain shall be regarded as a third country, if it is a member of the Single Euro Payments Area (SEPA), but not a Member State or an EEA member state. If a Member State concluded a bilateral agreement with a third country or a territory outside the Union in accordance with Article 24 of Regulation 2015/847/EU, the service provider located in that Member State may treat transfers of funds between that third country or territory and the Member State concerned as national transfers of funds.

10. For the purposes of applying Articles 5, 6 and 7 of Regulation 2015/847/EU, when calculating the EUR 1,000 threshold, the service provider shall consider the individual transfers of funds as a linked transaction if those are made from the same payment account to the same payment account or – when the transfer of funds is made not from a payment account to a payment account – they are made from the same payer to the same payee within an interval determined by the service provider in proportion to the ML/TF risk of the transaction, but maximum within one year.

11. The MNB regards it as good practice if the service provider defines other cases of transactions that appear to be linked considering the special features of its activity and customers.

12. The regulations and procedures developed by the service provider should be proportionate to the nature, size and complexity of the services provided by the service provider and should comply with the ML/TF risk existing in the case of the service provider, based on:

a) the nature of the customers it serves;

b) the nature of the products and services it provides;

c) the country in which it operates;

d) the sales channels it uses;

e) the number of service providers that regularly fail to provide the necessary information on the payer and payee;

f) the complexity of the payment chains in which it participates as a result of its business model;

g) the volume and amount of the transfers of funds performed by it; and

h) any other factors identified by the service provider during its AML/CFT activities and risk

assessment.

13. The MNB regards it as good practice if the service provider takes into consideration the provisions of MNB Recommendation No 7/2019 (IV. 1.) on assessing the risk of money laundering and terrorist financing associated with financial institutions and on determining related measures upon assessing the ML/TF risks.

14. The MNB expects the service provider to ensure that it has adequate resources to implement Regulation 2015/847/EU. In addition, the MNB specifically prescribes that persons directly or indirectly involved in AML/CFT tasks at the service provider should have adequate knowledge and understanding of the applicable AML/CFT legal, regulatory and procedural framework.

15. If the service provider uses an automated IT system procured from an external service provider, it should learn the operation and logic of the system in order to detect any errors in its efficient operation.

16. The MNB expects the service provider to develop regulations and procedures that clearly specify:

a) the criteria to be used for identifying which of its services and payment instruments fall within the scope of Regulation 2015/847/EU;

b) which of its services and payment instruments are covered by Regulation 2015/847/EU and which ones are not;

c) which transfers of funds should be monitored in real time and which can be monitored subsequently, and why;

d) the obligations and procedures to be followed by the relevant employee of the service provider if the information prescribed by Regulation 2015/847/EU is missing or incomplete;

e) the method and place of recording data on transfers of funds, the data to be attached to the transfer of funds in the payment chain and the data to be made available at the request of the payer's service provider;

f) the criteria that the relevant employees of the service provider should take into consideration when assessing whether the transfer of funds or other related transactions are suspicious or whether a notification is required under the provisions of the AML Act.

17. The service provider is expected to ensure that its regulations and procedures defining the detailed rules for the implementation of Regulation 2015/847/EU are approved by its manager specified in point 35 of Article 3 of the AML Act.

18. The service provider shall make available the regulations and procedures to all of its employees involved in the process. The service provider shall ensure that all relevant employees – particularly those involved in the implementation of Regulation 2015/847/EU and in the performance of the activities prescribed in the regulations – are familiar with the relevant provisions and ensure that they participate in the related training.

19. The MNB expects the service provider to review the regulations and procedures regularly, to amend them as necessary, also in view of possible changes in the ML/TF risks, and to keep them up-to-date. The service provider may also rely on its existing regulations and procedures in order to comply with the obligations under Regulation 2015/847/EU.

IV. Obligations of the payee's service providers

Verifying the permitted characters or input data

20. The MNB expects the service provider to monitor transfers of funds in real time and to check that the characters or input data used for entering payer and payee information comply with the rules of the messaging or payment and settlement system used for the execution of transfers of funds.

21. The service provider complies with the requirements prescribed in Article 7(1) and Article 11(1) of Regulation 2015/847/EU if it has ascertained and can prove to the MNB that it understands the

acceptance rules of the messaging or payment and settlement system and that this messaging or payment and settlement system

a) contains all fields necessary for obtaining the information prescribed by Regulation 2015/847/EU;

b) includes at least the payment account number or unique transaction identifier, which is suitable for tracing the transfer of funds back to the payer or payee;

c) automatically prevents the sending or receiving of transfers of funds if it detects unacceptable characters or input data; and

d) flags rejected transfers of funds for manual verification and processing.

For example, the service provider may regard the international bank account number (IBAN) or – if the transfer of funds is made by bankcard – the card number as a payment account number, if this information ensures the traceability of the transfer of funds back to the payer or payee.

22. If the messaging or payment and settlement system used by the service provider does not fulfil all the conditions specified in the previous section, the MNB expects the service provider to introduce controls to address the shortcomings.

Verification of missing data

23. Pursuant to Article 7(2) and Article 11(2) of Regulation 2015/847/EU, the service provider is expected to apply efficient procedures to detect possible missing information on the payer or payee which:

a) ensure the detection of meaningless or missing data;

b) include a combination of real-time monitoring and subsequent monitoring; and

c) ensure the identification high-risk factors.

Meaningless data

24. The service provider is expected to treat meaningless data as missing data. Examples of meaningless data include random character strings (e.g. "xxxxx" or "ABCDEFG") or obviously meaningless names (e.g. "Another" or "My Customer"), regardless of whether the data is entered using characters or input data that comply with the rules of the messaging or payment and settlement system.

25. Where the service provider chooses to list in its internal regulations the occurring meaningless data, the list shall be regularly reviewed and kept up-to-date. In this case, the service provider is not expected to check the transaction manually to identify meaningless data.

Real-time and subsequent monitoring

26. The MNB expects the service provider to perform monitoring activities in line with the ML/TF risks. The service provider shall take into consideration the risk factors described in sections 12 and 13 to ensure that its monitoring activities, including the level and frequency of subsequent and real-time monitoring, are proportionate to the identified ML/TF risk. In the course of this, the service provider shall identify the high-risk factors or combinations of individual risk factors that always require real-time monitoring or targeted subsequent monitoring. Real-time monitoring should be used when high-risk factors arise.

27. In addition to the real-time and targeted subsequent monitoring mentioned in the previous section, the service provider shall also carry out regular subsequent verifications on a random sample of all processed transfers of funds.

Factors indicating high risk

28 The service provider shall use systems that filter high-risk factors such as:

a) transfers of funds exceeding a certain threshold;

– when setting the threshold, the service provider shall take into consideration at least the average amount of the transfers of funds executed by it and the measure of unusually large transactions based on its business model,

b) a service provider with registered office, branch or business site in a country of high ML/TF risk or considered to be of high ML/TF risk due to other reason participates in the payment chain;

– the MNB expects the service provider to take into consideration the provisions of MNB Recommendation No 7/2019 (IV. 1.) when determining the countries of outstanding ML/TF risk,

c) a transfer of funds from a service provider that previously failed to provide the prescribed information on the payer without good cause several times or repeatedly (see sections 49–57);

d) a transfer of funds where the name of the payer or payee is missing;

e) the payer fails to provide the requested data despite repeated requests to this effect.

Management of transfers of funds with missing data or incorrectly provided data

29 To decide whether to reject, suspend or execute the transfer of funds in accordance with Articles 8 and 12 of Regulation 2015/847/EU, the service provider shall take into consideration the ML/TF risk associated with the transfer of funds, in particular:

a) whether the nature or uncommonness of the missing data gives rise to suspicion of ML/TF; and

b) whether one or more high-risk factors have been identified that may indicate that the transaction involves an outstanding ML/TF risk or that it is a suspected ML/TF transaction (see section 28).

30. Where the service provider monitors transfers of funds on a risk-sensitive basis subsequently in accordance with section 26 hereof, it shall apply the procedures specified in sections 37-39.

Refusal to execute the transfer of funds

31. If the service provider decides on refusing to execute the transfer of funds, it is not required to ask for the missing data, but it must inform the service provider preceding it in the payment chain of the reason for the refusal.

Suspension of the transfer of funds

32. If the service provider decides to suspend the transfer of funds, it shall notify the service provider preceding it in the payment chain to this effect and ask for the missing or incorrectly provided data.

33. A reasonable deadline shall be set for the provision of the missing or incorrect data, which shall not exceed three working days for transfers of funds between EEA member states and five working days for transfers of funds from non-EEA Member States. In the case of more complex payment chains, longer deadlines may be specified exceptionally.

34. If the necessary data are not received by the deadline, the service provider may send a reminder to the service provider preceding it in the payment chain with a warning that if the prescribed data are not received within the extended deadline, it will be flagged as a high-risk service provider in the future and treated as a recurrent defaulter under Article 8(2) of Regulation 2015/847/EU.

35. If the prescribed data are not received within the extended deadline, the service provider shall, in line with its risk-based regulations and procedures:

a) decide whether to reject or execute the transfer;

b) assess whether it gives rise to a suspicion that the service provider preceding it in the payment chain has not provided the prescribed data; and

c) assess how to treat the service provider preceding it in the payment chain in the future within the framework of preventing money laundering and terrorist financing.

36. The MNB expects the service provider to document and keep records of the measures taken and the reasons for taking or not taking measures under sections 32 to 35.

Execution of the transfer of funds

37. The MNB regards it as good practice if a service provider executes the transfer of funds, or subsequently notices that the prescribed data are missing or were provided using characters not permitted, it asks the service provider preceding it in the payment chain to provide the missing or incorrectly entered data.

38. If, in the course of real-time monitoring, the service provider finds that the prescribed data are missing and decides to execute the transfer after considering all relevant risks, it shall document the reasons for the execution of the respective transfer of funds.

39. The subsequent provision of missing date for transfers of funds executed despite missing or inadequate data shall be governed, mutatis mutandis by the provisions of sections 33–36 hereof.

Identifying and reporting suspicious transactions

40. The service provider shall assess whether the transfer is suspicious from an ML/TF point of view and, if so, whether it is justified to report it to the financial intelligence unit under the AML Act. Missing or incorrectly provided data alone may not be regarded as suspicious in terms of ML/TF.

41. When considering whether a particular transfer of funds is suspicious and requires reporting to the financial intelligence unit under the AML Act, the service provider shall perform a comprehensive inspection of all ML/TF risk factors associated with the transfer of funds, paying particular attention to transfers of funds that are likely to involve higher risk of ML/TF.

Recurrent defaulter service providers

42. In accordance with Articles 8(2) and 12(2) of Regulation 2015/847/EU, the MNB expects the service provider to develop procedures for the identification of "recurrent defaulter" service providers. To this end, it is necessary to keep a register of transfers of funds submitted with missing data.

43. The service provider may decide to treat a particular service provider as a "recurrent defaulter" for a number of reasons; however, for the justification of this decision a combination of quantitative and qualitative criteria should be taken into consideration with the details of the assessment specified in advance.

44. Quantitative criteria may include in particular:

a) the percentage of transfers sent by the respective service provider with missing or incorrect data within a specific period; and

b) the number of additional requests for data that were not answered or were answered incorrectly within the deadline.

45. The qualitative criteria for determining whether the service provider has defaulted recurrently shall include in particular:

a) the requested service provider's willingness to cooperate in connection with previous requests related to transfers sent with missing or incorrect data; and

b) the type of missing data, for example as indicated in section 28*d)*).

Reporting to the MNB

46. Once the service provider has established the existence of a recurrent omission in respect of a

service provider, it shall report it to the MNB, in addition to taking the measures specified in the regulations and procedures. The report shall include (in accordance with the Annex to this recommendation):

a) the name of the service provider who repeatedly failed to provide the data prescribed by the Regulation;

b) the country in which the activity of the recurrent defaulter service provider has been authorised;

c) the nature of the infringement, including in particular:

i) the frequency of transfers of funds sent with missing data,

ii) the period during which the infringements were identified, and

iii) a description of the recurrent omission and an explanation given by the defaulting service provider in this respect;

d) a description of the measures taken by the reporting service provider.

47. The reporting obligation detailed in the previous section shall not affect the reporting obligation to the financial intelligence unit pursuant to Articles 30–31 of the AML Act.

48. The report referred to in section 46 shall be made without undue delay, within maximum three months from identifying the service provider who has committed the recurrent omission.

Necessary steps

49 If a service provider repeatedly fails to send the information prescribed by Regulation 2015/847/EU, the other service provider participating in the payment chain shall take at least the following risk-based steps:

a) send a warning to the defaulting provider preceding it in the payment chain to inform it of the measures to be taken should the service provider continue to fail to send the data prescribed by the Regulation;

b) assess whether the repeated failure to send data by the service provider preceding it in the payment chain and its response to requests for missing information may affect the ML/TF risk linked to it and, if necessary, perform real-time monitoring of all transactions received from the defaulting service provider;

c) send a repeated warning to the service provider preceding it in the payment chain that all future transfers of funds will be rejected;

d) specify an extended deadline for the service provider preceding it in the payment chain, warning it that in the event of non-compliance it will reject all future transfers of funds; or

e) restrict or terminate its business relationship with the defaulting provider.

50. Before deciding to terminate the business relationship, the service provider shall assess whether it would be able to manage the risk adequately in any other way.

V. Additional obligations of the intermediary payment service provider

51. The intermediary payment service provider's systems are deemed adequate if they store all data accompanying the transfer of funds received by it and relating to the payer and payee together with the transfer in such a way that they can convert the data into another format without error or loss of data.

52. The intermediary payment service provider is expected to use only a payment or messaging system that allows the transmission of all data relating to the payer or payee, irrespective of whether the data are included in the data prescribed by Regulation 2015/847/EU. If this is not ensured, the intermediary payment service provider should implement some other method that ensures the transferring of all data to the payee's payment service provider.

VI. Additional obligations of the payee's payment service provider

Verification of data relating to the payee

53. Upon verifying the correctness of the data related to the payee in accordance with Article 7(3) and (4) of Regulation 2015/847/EU, the payment service provider shall apply the customer due diligence measures under the AML Act as long as its relationship with the payee qualifies as a business relationship under the AML Act.

54. The customer due diligence measures under the previous point may be waived if the verification of the identity of the payee and, where applicable, of the beneficial owner of the payee has already been carried out before 26 June 2017, in accordance with the provisions of the AML Act.

VII. Closing provisions

55. 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 enforcement practice as well as the methods, market standards and practices.

56. In line with the general European supervisory practice, during its audit and monitoring activity the MNB monitors and assesses compliance with the recommendation by the financial organisations supervised by it.

57. The MNB highlights that financial organisations may make the contents of this recommendation part of their policies. In such case, the financial organisation is entitled to indicate that the provisions of its relevant policies comply with the relevant recommendation issued by the MNB. If the financial organisation 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.

58. The MNB expects the respective financial institutions to apply this recommendation from 1 April 2020.

Annex 1 to MNB Decree No 1/2020 (III. 4.)

Notification template

Notification under Articles 8(2) and 12(2) of Regulation 2015/847/EU*	
PSP**/IPSP*** name:	
PSP/IPSP registered office:	
Date	
Name of the recurrent defaulter PSP/IPSP	
Identification of the country in which the recurrent defaulter PSP/IPSP has been authorised	
A brief description of the nature of the infringement and an explanation given by the recurrent defaulter PSP/IPSP for the infringement, if any	
Brief summary of the steps taken by the notifying PSP/IPSP to obtain the missing data.	

* For further information and guidance, see MNB Recommendation No 1/2020 (III. 4.) on procedures for the management of transfers of funds with missing data by payment service providers
** PSP – payment service provider
*** IPSP – intermediary payment service provider

CONTENTS

A tartalomjegyzék megjelenítéséhez kattintson a szürke hátterű szövegrészen jobb egér gombbal és válassza ki a Mező frissítése menüpontot.