FINANCIAL INTELLIGENCE ANALYSIS UNIT

GUIDANCE NOTE

ON

TRANSFERS OF FUNDS HAVING MISSING OR INCOMPLETE INFORMATION

A GUIDANCE NOTE ISSUED BY THE FIAU ON THE MEASURES PAYMENT SERVICE PROVIDERS SHOULD TAKE TO DETECT MISSING OR INCOMPLETE INFORMATION ON THE PAYER OR THE PAYEE, AND THE PROCEDURES THEY SHOULD PUT IN PLACE TO MANAGE A TRANSFER OF FUNDS LACKING THE REQUIRED INFORMATION

Issued: **25 October 2018**

Background information

1. Regulation (EU) 2015/847 sets out what are the obligations of Payment Service Providers ("PSPs") in relation to the information that is to accompany transfer of funds. This information is vital for the prevention, detection and investigation of money laundering and funding of terrorism ("ML/FT"). Being a regulation it is directly applicable and no transposition was necessary for its provisions to be applicable at national level.

2. In terms of Regulation 7(12) of the Prevention of Money Laundering and Funding of Terrorism Regulations ("PMLFTR"), subject persons carrying out relevant financial business involving the transfer of funds have to comply with the provisions of Regulation (EU) 2015/847. Failure to comply with this requirement is subject to administrative penalties imposed by the Financial Intelligence Analysis Unit ("FIAU") in terms of Regulation 21(2) of the PMLFTR.

3. On the 16 January 2018 the European Supervisory Authorities ("ESAs") published a series of guidelines on how a number of the provisions of Regulation (EU) 2015/847 are to be applied. These guidelines include measures that PSPs should take to detect missing or incomplete information on the payer or the payee, and the procedures they should put in place to manage a transfer of funds lacking the required information.

4. The FIAU has taken note of the said guidelines and, in line with its functions at law, it is issuing the present Guidance Note to ensure that local PSPs are all aware of the ESAs guidelines and are provided with guidance on how to implement their obligations under the said Regulation and especially under Article 7, Article 8, Article 11 and Article 12 of the same.

5. This Guidance Note is being issued in terms of Regulation 17 of the PMLFTR. As such, it is binding on all subject persons concerned and enforceable by the FIAU. Any failure to comply with guidance issued by the FIAU in accordance with the aforementioned provision is subject to the applicable administrative penalties.

Purpose and Scope

6. This Guidance Note is addressed to PSPs where they act either as the PSP of the payee or as intermediary payment service providers ("IPSPs") as defined in point (6) of Article 3 of Regulation (EU) 2015/847. Its purpose is to:

    a. Help PSPs and IPSPs determine which transfers of funds are within the scope of Regulation (EU) 2015/847, and how to benefit from the exemptions provided for under Article 2 of the mentioned Regulation and expressly referred to in this Guidance Note;

    b. Provide PSPs and IPSPs with tools to establish and implement effective procedures to detect transfers of funds that lack required information on the payer or the payee, and to follow up should this be necessary; and

    c. Set out the risk factors PSPs and IPSPs should consider when determining whether to execute, reject or suspend a transfer of funds which lacks required information on the

payer or the payee, including when assessing whether or not the lack of information gives rise to knowledge, suspicion or reasonable grounds to suspect of ML/TF.

General Considerations

7. A PSP has to establish for each transfer of funds whether it is acting as the PSP of the payer, as the PSP of the payee or as an IPSP. This will determine what information has to accompany a transfer of funds and the steps the PSP or IPSP has to take to comply with Regulation (EU) 2015/847.

   Where a transfer of funds is a direct debit as defined in point (9)(b) of Article 3 of Regulation (EU) 2015/847, the PSP of the payee is to send the required information on the payer and the payee to the PSP of the payer as part of the direct debit collection. The PSP of the payee and the IPSP may then assume that the information requirements in point (2) and (4) of Article 4 and points (1) and (2) of Article 5 of Regulation (EU) 2015/847 are met.

Exemptions and Derogations

8. PSPs and IPSPs must comply with Regulation (EU) 2015/847 in respect of all transfers of funds that are at least partly carried out by electronic means and irrespective of the messaging or payment and settlement system used, unless the transfer qualifies for any of the exemptions and/or derogations set out in Regulation (EU) 2015/847 referred to hereunder.

9. To apply these exemptions and derogations, PSPs and IPSPs must have in place systems and controls to ensure they meet the conditions for these exemptions and derogations. PSPs and IPSPs that are unable to establish whether the conditions for these exemptions are met or otherwise have to comply in full with all the obligations arising from Regulation (EU) 2015/847 in respect of all transfers of funds.

   Article 5 of Regulation (EU) 2015/847

10. In order to apply the derogation in Article 5 of Regulation (EU) 2015/847:

    a. PSPs of the payee have to be able to determine that the PSP of the payer is based in the European Economic Area ("EEA"); and

    b. IPSPs have to be able to determine that the PSP of the payer and the PSP of the payee are based in the EEA.

    Countries which form part of the Single Euro Payments Area but are not part of the EEA are to be treated as third countries.

    Article 2(3) of Regulation (EU) 2015/847

11. When applying the exemption in point (3) of Article 2 of Regulation (EU) 2015/847, PSPs and IPSPs are to ensure that the transfer of funds is accompanied by the number of the card, instrument or digital device, for example the Primary Account Number (PAN), and that that number is provided in a way that allows the transfer to be traced back to the payer.

12. Where the card, instrument or device can be used to effect both person-to-person transfers of funds and payments for goods or services, PSPs and IPSPs will be able to apply this

exemption only if they are able to determine that the transfer of funds is not a person-to person transfer of funds, but constitutes a payment for goods or services instead.

Articles 5, 6 and 7 of Regulation (EU) 2015/847

13. In order to apply the rules in Articles 5, 6 and 7 of Regulation (EU) 2015/847 related to transfers of funds that do not exceed EUR 1 000, PSPs and IPSPs should have in place measures, policies, controls and procedures to detect transfers of funds that appear to be linked. PSPs and IPSPs are to treat transfers of funds as linked if these fund transfers are being sent:

    a. From the same payment account to the same payment account, or, where the transfer is not made to or from a payment account, from the same payer to the same payee; and

    b. Within a reasonable, short timeframe, which should be set by the PSP in a way that is commensurate with the ML/TF risk to which their business is exposed.

    PSPs and IPSPs should determine whether other scenarios might also give rise to linked transactions and, if so, reflect these in their policies and procedures.

Measures, Policies, Controls and Procedures

14. PSPs and IPSPs are reminded of their obligations under Regulation 5(5) of the PMLFTR whereby they must have in place and implement measures, policies, controls and procedures proportionate to the nature and size of their business and which address the risks identified as a result of their business risk assessment.

15. The risks that PSPs and IPSPs have to consider include:

    a. The risks indicated in the Implementing Procedures – Part I issued by the FIAU;

    b. The risks indicated by the ESAs in their *Joint Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 on simplified and enhanced customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions* and available through https://esas-joint-committee.europa.eu/Pages/Guidelines/Joint-Guidelines-on-Risk-Factors.aspx ;

    c. The number of PSPs and IPSPs regularly failing to provide required information on the payer and the payee;

    d. The complexity of the payment chains in which it intervenes as a result of its business model; and

    e. The volume and value of transactions it processes.

16. Without prejudice to their obligations under the PMLFTR, PSPs and IPSPs are to ensure that their measures, policies, controls and procedures:

    a. Set out clearly:

i. Which criteria they use to determine whether or not their services and payment instruments fall under the scope of Regulation (EU) 2015/847,

ii. Which of their services and payment instruments fall within the scope of Regulation (EU) 2015/847 and which do not,

iii. Which transfers of funds have to be monitored in real time and which transfers of funds can be monitored on an ex-post basis, together with the reasons for any such decision,

iv. The obligations of their officials and employees where they detect that information required by Regulation (EU) 2015/847 is missing and the processes they should follow, and

v. Which information relating to transfers of funds has to be recorded, how this information should be recorded, and where it is to be kept;

b. Are approved by the PSP's or IPSP's senior management as set out in Regulation 5(6) of the PMLTR;

c. Are available to all relevant officials and employees, including persons responsible for processing transfers of funds. PSPs and IPSPs are to ensure that all relevant staff members are appropriately trained in the application of these policies and procedures; and

d. Are reviewed regularly, improved where necessary and kept up to date. PSPs may draw on existing policies and procedures to meet their obligations under Regulation (EU) 2015/847 where possible.

Obligations on IPSPs and PSPs of the Payee

Admissible Characters or Inputs Checks - Article 7(1) and Article 11(1) of Regulation (EU) 2015/847)

17. PSPs and IPSPs are to monitor transfers of funds to detect whether or not the characters or inputs used to provide information on the payer and the payee comply with the conventions of the messaging or payment and settlement system that was used to process the transfer of funds.[1] These checks should be carried out in real time.

18. PSPs and IPSPs may assume that they comply with point (1) of Article 7 and point (1) of Article 11 of Regulation (EU) 2015/847 respectively if they are satisfied, and can demonstrate to the Financial Intelligence Analysis Unit, that they understand the messaging or payment and settlement system's validation rules and that the conventions of that system mean that it:

[1] Articles 7(1) and 11 (1) of Regulation (EU) 2015/847.

a. Contains all the fields necessary to obtain the information required by Regulation (EU) 2015/847. For example, PSPs and IPSPs may treat the International Bank Account Number (IBAN) or, where the transfer of funds is made using a payment card, the number of that card (for example the PAN) as the payment account number on condition that the number used permits the fund transfer to be traced to the payer or the payee;

b. Automatically prevents the sending or receiving of transfers of funds where inadmissible characters or inputs are detected; and

c. Flags rejected transfers of funds for manual review and processing.

Where a PSP's or IPSP's messaging, or payment and settlement system does not meet all the criteria stipulated hereabove, the PSP or IPSP are to put in place controls to mitigate the shortcomings.

Missing Information Checks - Article 7(2) and Article 11(2) of Regulation (EU) 2015/847)

19. PSPs and IPSPs must implement effective procedures to detect if the required information on the payer or the payee is missing, i.e. the information on the payer or the payee required by Regulation (EU) 2015/847 has not been provided. To be effective, these procedures should

    a. Enable the PSP or IPSP to spot meaningless information;

    b. Employ a combination of real-time monitoring and ex-post monitoring; and

    c. Alert the PSP or IPSP to high-risk indicators.

20. PSPs and IPSPs are to treat meaningless information as though it were missing information. Examples of meaningless information include strings of random characters (e.g. 'xxxxx', or 'ABCDEFG') or designations that clearly make no sense (e.g. 'An Other', or 'My Customer'), even if this information has been provided using characters or inputs in accordance with the conventions of the messaging or payment and settlement system.

21. Where PSPs or IPSPs use a list of commonly found meaningless terms, they are to periodically review this list to ensure it remains relevant. In those cases, there is no expectation that PSPs or IPSPs manually review all transactions to detect meaningless information.

22. PSPs and IPSPs are to refer to the risk factors specified in point 15 to ensure that their approach to monitoring, including the level and frequency of ex-post and real-time monitoring, is commensurate with the ML/TF risk to which they are exposed. As part of this, PSPs and IPSPs must determine which high-risk factors, or combination of high-risk factors, will always trigger real-time monitoring, and which will trigger a targeted *ex-post* review (see also point 26). In cases of specific concern, transfers of funds are always be monitored in real time.

23. Real-time monitoring refers to monitoring performed either before the funds are credited to the payee's payment account with the PSP of the payee or, where the payee does not have a payment account with the PSP of the payee, before the funds are made available to the payee by the PSP that receives the funds. In the case of an IPSP, real-time monitoring refers to the monitoring performed before the IPSP transfers the funds on behalf of the PSP of the payer or of another IPSP.

24. *Ex-post* monitoring refers to monitoring performed after the funds have been credited to the payee's payment account with the PSP of the payee or, where the payee does not have a payment account with the PSP of the payee, after the funds have been made available to the payee by the PSP of the payee, or transmitted by the IPSP. In the case of an IPSP, ex-post monitoring refers to the monitoring performed after the IPSP has transferred the funds on behalf of the PSP of the payer or of another IPSP.

25. In addition to real-time and targeted *ex-post* monitoring in point 22, PSP and IPSP are also to perform on a regular basis ex-post reviews on a random sample taken from all processed transfers of funds.

26. PSPs' and IPSPs' systems should be configured in a way that alerts are triggered should a high-risk indicator be detected. High-risk indicators may include, but are not limited to:

    a. Transfers of funds that exceed a specific value threshold. When deciding on the threshold, PSPs and IPSPs should at least consider the average value of transactions they routinely process and what constitutes an unusually large transaction, taking into account the particular business model adopted by the given PSP or IPSP;

    b. Transfers of funds where the PSP of the payer or the PSP of the payee is based in a high risk or non-reputable jurisdiction. When identifying high risk jurisdictions, PSPs and IPSPs should have regard to the relevant sections of the Implementing Procedures and to the ESAs' Risk Factors Guidelines;

    c. A negative AML/CFT compliance record of the IPSP or the PSP of the payer, whoever is the prior PSP in the payment chain;

    d. Transfers of funds from a PSP or IPSP identified as repeatedly failing to provide required information on the payer without good reason (see points 41-48), or from a PSP or IPSP that has previously been known to fail to provide required information on the payer or the payee on a number of occasions without good reason, even if it did not repeatedly fail to do so; and

    e. Transfers of funds where the name of the payer or the payee is missing.

Managing Transfers of Funds with Missing Information, or Inadmissible Characters or Inputs - Article 8 and Article 12 of Regulation (EU) 2015/847

27. PSPs and IPSPs are to have in place effective risk-based procedures to determine whether to execute, reject or suspend a transfer of funds where real-time monitoring reveals that the required information on the payer or the payee is missing or provided using inadmissible characters or inputs.

28. In order to determine whether to reject, suspend or execute a transfer of funds in compliance with Articles 8 and 12 of Regulation (EU) 2015/847, PSPs and IPSPs are to consider the ML/TF risk associated with that transfer of funds before deciding on the appropriate course of action. PSPs and IPSPs should consider in particular whether or not:

    a. The type of information missing gives rise to ML/TF concerns; and

b. One or more high-risk indicators have been identified that may suggest that the transaction presents a high ML/TF risk or gives rise to knowledge or suspicion of, or reasonable grounds to suspect, ML/TF (see point 26).

Where PSPs or IPSPs have taken a risk-sensitive decision, in line with point 22 of the Guidance Note, to monitor transfers of funds ex post, they should follow the guidance in points 35-39.

29. Where a PSP or an IPSP decides to reject a transfer of funds, it does not have to ask for the missing information but should share the reason for the rejection with the prior PSP in the payment chain.

30. Where a PSP or an IPSP decides to suspend the transfer of funds, it is to notify the prior PSP in the payment chain that the transfer of funds has been suspended and ask the prior PSP in the payment chain to supply the information on the payer or the payee that is missing, or to provide that information using admissible characters or inputs.

31. When asking for missing information, the PSP or IPSP should set the prior PSP in the payment chain a reasonable deadline by which the information should be provided. This deadline should not normally exceed three (3) working days for transfers of funds taking place within the EEA, and five (5) working days for transfers of funds received from outside the EEA. Longer deadlines may be necessary where payment chains are more complex.

32. PSPs or IPSPs should consider sending a reminder to the prior PSP in the payment chain should the requested information not be forthcoming. As part of this, a PSP or IPSP may decide to advise the prior PSP in the payment chain that, if the required information is not received before an additional deadline, the prior PSP in the payment chain may be subject to internal high-risk monitoring (see point 26) and treated as repeatedly failing, as set out in point (2) of Article 8 of Regulation (EU) 2015/847.

33. Where the requested information is not provided by the set deadline, the PSP or IPSP should, in line with its risk-based policies and procedures:

    a. Decide whether to reject or execute the transfer;

    b. Consider whether or not the prior PSP in the payment chain's failure to supply the required information gives rise to suspicion; and

    c. Consider the future treatment of the prior PSP in the payment chain for AML/CFT compliance purposes.

34. PSPs and IPSPs should document and record all of these actions and the reason for their actions or inaction, and make the same available to the Financial Intelligence Analysis Unit or relevant supervisory authority upon demand.

The PSP or IPSP Executes the Transfer

35. Where a PSP or IPSP executes the transfer of funds, or detects *ex post* that required information was missing or provided using inadmissible characters, it is to ask the prior PSP in the payment chain to provide the missing information on the payer or the payee, or to provide that information using admissible characters or inputs after the transfer has been executed.

36. A PSP or IPSP that becomes aware that required information is missing while carrying out real-time monitoring, but decides to execute the transfer of funds having considered all relevant risks, is to document the reason for executing that transfer.

37. When asking for missing information, the PSP or IPSP is to proceed in line with point 32 of this Guidance Note.

38. Where the requested information is not forthcoming within the timeframe set by the PSP or IPSP, the PSP or IPSP should, in line with its risk-based measures, policies, controls and procedures, consider the future treatment of the prior PSP in the payment chain for AML/CFT compliance purposes.

39. The PSP or IPSP is to document and record all of these actions and the reason for their actions or inaction, and make the same available to the Financial Intelligence Analysis Unit or relevant supervisory authority upon demand.

Identifying and Reporting Suspicious Transactions - Article 9 and Article 13 of Regulation (EU) 2015/847

40. PSPs and IPSPs are reminded of their reporting obligations under Regulation 15 of the PMLFTR which are equally applicable in relation to a transfer of funds. PSPs and IPSPs should note that missing or inadmissible information may not, by itself, give rise to knowledge or suspicion of, or reasonable grounds to suspect, ML/TF. A PSP or IPSP should take a holistic view of all ML/TF risk factors associated with the transfer of funds, including those listed in point 26, to the extent that these are known, and pay particular attention to transfers of funds that are likely to present a higher risk of ML/TF.

Repeatedly Failing PSPs or IPSP and Steps to be Taken - Article 8(2) and Article 12 (2) of Regulation (EU) 2015/847

41. PSPs and IPSPs are to put in place measures, policies, controls and procedures to identify PSPs and IPSPs that repeatedly fail to provide the required information on the payer or the payee. To this end, PSPs and IPSPs have to keep a record of all transfers of funds with missing information to be able to determine which PSPs or IPSPs should be classified as 'repeatedly failing'.

42. A PSP or IPSP may decide to treat a PSP or IPSP as 'repeatedly failing' for various reasons, but should consider a combination of quantitative and qualitative criteria to inform that decision.

43. Quantitative criteria for assessing whether or not a PSP or IPSP is repeatedly failing include the percentage of:

    a. Transfers with missing information sent by a specific PSP or IPSP within a certain timeframe; and

    b. Follow-up requests that were left unanswered or were not adequately answered by a certain deadline.

44. Qualitative criteria for assessing whether or not a PSP or IPSP is repeatedly failing include:

a. The level of cooperation of the requested PSP or IPSP relating to previous requests for missing information; and

b. The type of information missing (see, for example, point 26 e).

45. Once a PSP or IPSP has identified another PSP or IPSP as repeatedly failing to provide required information, a notification is to be sent to the Financial Intelligence Analysis Unit using the form set out in Annex A to this Guidance Note. This notification is to be sent on the following email address: compliance@fiumalta.org. In exceptional circumstances, the Financial Intelligence Analysis Unit will also accept notifications in writing. When describing the nature of the breach, it is important that the PSP or IPSP filing the notification provides information relative to:

    a. The frequency of transfers of funds with missing information;
    b. The period of time during which the breaches were identified; and
    c. Any reasons the PSP or IPSP may have given to justify their repeated failure to provide the required information.

    This notification requirement is without prejudice to the reporting obligations arising from Regulation 15 of the PMLFTR.

46. PSPs and IPSPs are to notify the Financial Intelligence Analysis Unit upon identifying a repeatedly failing PSP or IPSP without undue delay, and no later than three (3) months after identifying the repeatedly failing PSP or IPSP. The Financial Intelligence Analysis Unit will then notify the EBA.

47. The steps the PSP of the payee or the IPSP is to take where another PSP or IPSP repeatedly fails to provide information required by Regulation (EU) 2015/847 should be risk-based and may include one or a combination of the following (though other steps are possible):

    a. Issuing a warning to the prior PSP in the payment chain to inform the PSP or IPSP of the steps that will be applied should the PSP continues to fail to provide the information required by Regulation (EU) 2015/847;

    b. Considering how the repeated failure by the prior PSP in the payment chain to provide information and that PSP's attitude to responding to such requests affects the ML/TF risk associated with that PSP, and where appropriate, carrying out real-time monitoring of all transactions received from that PSP;

    c. Issuing a further warning to the prior PSP in the payment chain that it will reject any future transfers of funds;

    d. Restricting or terminating the business relationship with the failing PSP.

48. Before taking the decision to terminate a business relationship, in particular where the prior PSP in the payment chain is a respondent bank from a third country, the PSP or IPSP should consider whether or not it can manage the risk in other ways, including through the application of enhanced due diligence measures as provided for under Regulation 11 of the PMLFTR.

Additional Obligations for the IPSP

49. IPSPs should satisfy themselves that their systems and controls enable them to comply with their duty to ensure that all information on the payer and the payee that accompanies a transfer of funds is retained with that transfer. As part of this obligation, IPSPs should satisfy themselves of their system's ability to convert information into a different format without error or omission.

50. IPSPs should use only payment or messaging systems that permit the onward transfer of all information on the payer or the payee, irrespective of whether or not this information is required by Regulation (EU) 2015/847. Where this is not possible, for example because a domestic payment system restricts the data that can be entered into that system, IPSPs should put in place alternative mechanisms to pass on relevant information to the PSP of the payee.

Additional obligations for the PSP of the payee

Incomplete Information

51. PSPs of the payee are to also apply the provisions of paragraphs 17 to 48 of this Guidance Note also in relation to information that is incomplete. Incomplete information refers to information on the payer or the payee required by Regulation (EU) 2015/847 that has been provided only in part

Verification of Information on the Payee

52. Regulation (EU) 2015/847 also requires that the information collected on the payee is verified for its accuracy. This is to be done by applying the measures set out in the Implementing Procedures to give effect to the verification of identity obligations arising from Regulation 7(1)(a). However, where the transfer of funds takes place within a business relationship, the PSP need not verify the information each time that a transfer of funds takes place but should be so done on the same basis as set out in Regulation 7(6) of the PMLFTR.

Record-keeping

53. In line with Article 16 of Regulation (EU) 2015/847, PSPs must retain records of information on the payer and the payee that they receive in line with Articles 4 to 7 of the said Regulation. This is to be done in line with what is provided for under Regulation 16 of the PMLFTR.

Conclusion

54. This Guidance Note is to be read together with the Guidelines issued by the ESAs, which are accessible through the following link:

    https://esas-joint-committee.europa.eu/Pages/Guidelines/Joint-Guidelines-to-prevent-terrorist-financing-and-money-laundering-in-electronic-fund-transfer.aspx

    Furthermore, it should be noted that Regulation (EU) 2015/847 and this Guidance Note are without prejudice to any other obligation that PSPs in general may be subject to in terms of

the Prevention of Money Laundering Act[2], the PMLTR and any Implementing Procedures issued by the Financial Intelligence Analysis Unit from time to time.

55. Any questions or clarifications in relation to the contents of this Guidance Note may be addressed to the FIAU.

Email: info@fiumalta.org
Tel: +356 21 231 333

[2] Cap 373 of the Laws of Malta.

Annex A — Notification Template

Notification pursuant to point (2) of Article 8 of Regulation (EU) 2015/847	
Name of reporting PSP/IPSP	
Address of reporting PSP/IPSP	
Date	
Name of repeatedly failing PSP/IPSP	
Name of country in which the repeatedly failing PSP/IPSP is authorised	
Short description of the nature of the breach and reasons given by the repeatedly failing PSP/IPSP, if any, to justify that breach	
Short summary of the steps the reporting PSP/IPSP has taken to obtain missing information.	