JC/GL/2017/16

16/01/2018

Final Guidelines

Joint Guidelines under Article 25 of Regulation (EU) 2015/847 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

Joint Guidelines under Article 25 of Regulation (EU) 2015/847 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

Status of these joint guidelines

This document contains joint guidelines issued pursuant to Articles 16 and 56, subparagraph 1, of Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC; Regulation (EU) No 1094/2010 establishing a European Supervisory Authority (European Insurance and Occupational Pensions Authority); and Regulation (EU) No 1095/2010 establishing a European Supervisory Authority (European Securities and Markets Authority): 'the ESAs' Regulations'. In accordance with Article 16(3) of the ESAs' Regulations, competent authorities and financial institutions must make every effort to comply with the guidelines.

Joint guidelines set out the ESAs' view of appropriate supervisory practices within the European System of Financial Supervision or of how Union law should be applied in a particular area. Competent authorities to whom the joint guidelines apply should comply by incorporating them into their supervisory practices as appropriate (e.g. by amending their legal framework or their supervisory processes), including where the joint guidelines are directed primarily at institutions.

Reporting requirements

In accordance with Article 16(3) of the ESAs' Regulations, competent authorities must notify the respective ESA whether they comply or intend to comply with these Joint Guidelines, or otherwise with reasons for non-compliance, by 16/03/2018 (two months after issuance). In the absence of any notification by this deadline, competent authorities will be considered by the respective ESA to be non-compliant. Notifications should be sent to [compliance@eba.europa.eu, compliance@eiopa.europa.eu and compliance@esma.europa.eu] with the reference 'JC/GL/2017/16'. A template for notifications is available on the ESAs' websites. Notifications should be submitted by persons with appropriate authority to report compliance on behalf of their competent authorities.

Notifications will be published on the ESAs' websites, in line with Article 16(3) of the ESAs' Regulations.

Title I — Subject matter, scope and definitions

Subject matter and scope

1. These guidelines are addressed to:

   a) payment service providers (PSPs) as defined in point (5) of Article 3 of Regulation (EU) 2015/847 where they act as the PSP of the payee, and intermediary payment service providers (IPSPs) as defined in point (6) of Article 3 of Regulation (EU) 2015/847; and

   b) competent authorities responsible for supervising PSPs and IPSPs for compliance with their obligations under Regulation (EU) 2015/847.

2. These guidelines:

   a) set out the factors PSPs and IPSPs should consider when establishing and implementing procedures to detect and manage transfers of funds that lack required information on the payer and/or the payee to ensure that these procedures are effective; and

   b) specify what PSPs and IPSPs should do to manage the risk of money laundering (ML) or terrorist financing (TF) where the required information on the payer and/or the payee is missing or incomplete.

3. Competent authorities should use these guidelines when assessing the adequacy of the procedures and measures adopted by PSPs and IPSPs to comply with Articles 7, 8, 11 and 12 of Regulation (EU) 2015/847.

4. PSPs, IPSPs and competent authorities should also use these guidelines to ensure compliance with Articles 9 and 13 of Regulation (EU) 2015/847.

5. The factors and measures described in these guidelines are not exhaustive. PSPs and IPSPs should consider other factors and measures as appropriate.

6. These guidelines do not apply to restrictive measures imposed by regulations based on Article 215 of the Treaty on the Functioning of the European Union, such as Regulations (EC) No 2580/2001, (EC) No 881/2002 and (EU) No 356/2010 (‘the European sanctions regime’).

Definitions

7. Unless otherwise specified, the terms used and defined in Directive (EU) 2015/849 and in Regulation (EU) 2015/847 have the same meaning in these guidelines. In addition, for the purposes of these guidelines, the following definitions apply:

a) 'competent authorities' means the authorities responsible for ensuring PSPs' and IPSPs' compliance with the requirements of Regulation (EU) 2015/847;

b) 'risk' means the impact and likelihood of ML/TF taking place;

c) 'risk factors' means variables that, either on their own or in combination, may increase or decrease the ML/TF risk posed by an individual business relationship, occasional transaction or fund transfer;

d) 'risk-based approach' means an approach whereby competent authorities, PSP and IPSP identify, assess and understand the ML/TF risks to which PSP and IPSP are exposed and take AML/CFT measures that are proportionate to those risks;

e) 'missing information' means information on the payer or the payee as required by Regulation (EU) 2015/847 that has not been provided;

f) 'incomplete information' means information on the payer or the payee as required by Regulation (EU) 2015/847 that has been provided only in part;

g) 'real-time monitoring' refers to monitoring performed:

   i) before the funds are credited to the payee's payment account with the PSP of the payee,

   ii) 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 or

   iii) where the PSP is an IPSP, before the IPSP transfers the funds on behalf of the PSP of the payer or of another IPSP;

h) 'ex-post monitoring' refers to monitoring performed:

   i) after the funds have been credited to the payee's payment account with the PSP of the payee,

   ii) 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 or

   iii) where the PSP is an IPSP, after the IPSP has transferred the funds on behalf of the PSP of the payer or of another IPSP.

Title II – Detecting missing information and managing transfers of funds with missing information

CHAPTER I: General considerations

Establishing obligations under Regulation (EU) 2015/847

8. A PSP should establish for each transfer of funds whether it acts 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.

Direct debits

9. 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 should send 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.

Applying derogations and exemptions under Regulation (EU) 2015/847

10. 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 Regulation (EU) 2015/847 sets out exemptions and derogations.

11. To apply these exemptions and derogations, PSPs and IPSPs should have in place systems and controls to ensure the conditions for these exemptions and derogations are met. PSPs and IPSPs that are unable to establish that the conditions for these exemptions are met should comply with Regulation (EU) 2015/847 in respect of all transfers of funds.

Article 5 of Regulation (EU) 2015/847

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

    a) PSPs of the payee should be able to determine that the PSP of the payer is based in the Union or an EEA Member State; and

    b) IPSPs should be able to determine that the PSP of the payer and the PSP of the payee are based in the Union or an EEA Member State.

13. PSPs and IPSPs should treat countries as third countries if they are part of the Single Euro Payments Area (SEPA) but are not also Member States of the Union or EEA. Where a Member State has concluded a bilateral agreement with a third country or territory

outside the Union in accordance with Article 24 of Regulation (EU) 2015/847, PSPs and IPSPs in that Member State may treat transfers of funds from or to that third country or territory as domestic transfers of funds.

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

14. When applying the exemption in point (3) of Article 2 of Regulation (EU) 2015/847, PSPs and IPSPs should 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.

15. 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

16. In order to apply 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 policies and procedures to detect transfers of funds that appear to be linked. PSPs and IPSPs should 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.

17. 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.

Proportionality and business-wide risk assessments

18. PSPs and IPSPs should establish and maintain effective policies and procedures to comply with Regulation (EU) 2015/847. These policies and procedures should be proportionate to the nature, size and complexity of the PSP's or IPSP's business, and commensurate with the ML/TF risk to which the PSP or IPSP is exposed as a result of:

    a) the type of customers it services;

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

    c) the jurisdictions it services;

d) the delivery channels it uses;

e) the number of PSPs and IPSPs regularly failing to provide required information on the payer and the payee;

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

g) the volume and value of transactions it processes.

19. When assessing the ML/TF risk to which they are exposed, PSPs and IPSPs should refer to the ESAs' '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' (the Risk Factors Guidelines).[1]

Policies and procedures

20. PSPs and IPSPs should ensure that their policies 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, and why,

iv) the obligations of members of staff 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;

b) are approved by the PSP's or IPSP's senior management, as defined in point (12) of Article 3 of Directive (EU) 2015/849;

c) are available to all relevant members of staff, including persons responsible for processing transfers of funds; PSPs and IPSPs should ensure that all relevant staff

[1] https://esas-joint-committee.europa.eu/Pages/Guidelines/Joint-Guidelines-on-Risk-Factors.aspx

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.

CHAPTER II: 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)

21. PSPs and IPSPs should 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.[2] These checks should be carried out in real time.

22. 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 their competent authority, that they understand the messaging or payment and settlement system's validation rules and that the conventions of that system mean that it:

    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.

23. Where a PSP's or IPSP's messaging, or payment and settlement system does not meet all the criteria stipulated in point 22 of these guidelines, the PSP or IPSP should put in place controls to mitigate the shortcomings.

Missing information checks
(Article 7(2) and Article 11(2) of Regulation (EU) 2015/847)

Effective procedures

24. PSPs and IPSPs must implement effective procedures to detect if the required information on the payer or the payee is missing.[3]

25. To be effective, these procedures should

    a) enable the PSP or IPSP to spot meaningless information;

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

[3] Articles 7(2) and 11(2) of Regulation (EU) 2015/847.

b) employ a combination of real-time monitoring and ex-post monitoring; and

c) alert the PSP or IPSP to high-risk indicators.

Meaningless information

26. PSPs and IPSPs should treat meaningless information as though it was 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.

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

Real-time and ex-post monitoring

28. PSPs and IPSPs should refer to the risk factors specified in point 18 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 should 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 30). In cases of specific concern, transfers of funds should always be monitored in real time.

29. In addition to real-time and targeted ex-post monitoring in point 28, PSP and IPSP should regularly perform ex-post reviews on a random sample taken from all processed transfers of funds.

High-risk indicators

30. PSPs' and IPSPs' systems should be configured in a way that triggers alerts 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 their particular business model;

b) transfers of funds where the PSP of the payer or the PSP of the payee is based in a country associated with high ML/TF risk, including, but not limited to, countries identified as high risk by the European Commission in accordance with Article 9 of Directive (EU) 2015/849. When identifying countries associated with high ML/TF risk, PSPs and IPSPs should have regard 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 47-55), 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;

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)

31. PSPs and IPSPs should put 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.

32. 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 should 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 suspicion of ML/TF (see point 30).

    Where PSPs or IPSPs have taken a risk-sensitive decision, in line with point 28 of these guidelines, to monitor transfers of funds ex post, they should follow the guidance in points 40-43.

    The PSP or IPSP rejects the transfer

33. 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.

    The PSP or IPSP suspends the transfer

34. Where a PSP or an IPSP decides to suspend the transfer of funds, it should 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.

35. 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 working days for transfers of funds taking

place within the EEA, and five working days for transfers of funds received from outside the EEA. Longer deadlines may be necessary where payment chains are more complex.

36. 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 30) and treated as repeatedly failing, as set out in point (2) of Article 8 of Regulation (EU) 2015/847.

37. 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.

38. PSPs and IPSPs should document and record all of these actions and the reason for their actions or inaction, so that they are later capable of responding to possible requests by the competent authorities for information about compliance with legally binding acts of the Union, for example where, as a result of actions taken under Article 8 of Regulation (EU) 2015/847, the PSP or IPSP has been unable to comply with relevant obligations in Articles 83 and 84 of Directive (EU) 2015/2366 as incorporated into the applicable national legal framework.

The PSP or IPSP executes the transfer

39. 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 should 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.

40. 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, should document the reason for executing that transfer.

41. When asking for missing information, the PSP or IPSP should proceed in line with point 36 of these guidelines.

42. 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 policies and procedures, consider the future treatment of the prior PSP in the payment chain for AML/CFT compliance purposes.

43. The PSP or IPSP should document and record all of these actions and the reason for their actions or inaction, so that they are later capable of responding to possible requests of the authorities.

Identifying and reporting suspicious transactions (Article 9 and Article 13 of Regulation (EU) 2015/847)

44. PSPs and IPSPs should assess whether or not a transfer of funds is suspicious, taking into account any criteria set out in Union law, national legislation and their own, internal AML/CFT policies and procedures.

45. PSPs and IPSPs should note that missing or inadmissible information may not, by itself, give rise to suspicion of ML/TF. When considering whether or not a transfer of funds raises suspicion, the 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 30, 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.

46. PSPs and IPSPs should be able to demonstrate that they comply with directly applicable Union law and national legislation in the area of AML/CFT. In some cases, national legislation may require them to take additional action, for example the reporting of unusual transactions that may not give rise to suspicion 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)

When is a PSP or IPSP considered to be 'repeatedly failing' to provide required information?

47. PSPs and IPSPs should put in place policies and procedures to identify PSPs and IPSPs that repeatedly fail to provide the required information on the payer or the payee.

48. To this end, PSPs and IPSPs should keep a record of all transfers of funds with missing information to be able to determine which PSP or IPSP should be classified as 'repeatedly failing'.

49. 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.

50. Quantitative criteria for assessing whether or not a PSP or IPSP is repeatedly failing include:

    a) the percentage of transfers with missing information sent by a specific PSP or IPSP within a certain timeframe; and

    b) the percentage of follow-up requests that were left unanswered or were not adequately answered by a certain deadline.

51. 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 30 e).

Notifying the authorities

52. Once a PSP or IPSP has identified another PSP or IPSP as repeatedly failing to provide required information, a notification to the authorities specified in the second subparagraph of Article 8(2) of Regulation (EU) 2015/847 should include, in line with the Annex to these guidelines:

    a) the name of the PSP or IPSP identified as repeatedly failing to provide the required information;

    b) the country in which the PSP or IPSP is authorised;

    c) the nature of the breach, including:

        i) the frequency of transfers of funds with missing information,

        ii) the period of time during which the breaches were identified and

        iii) any reasons the PSP or IPSP may have given to justify their repeated failure to provide the required information;

    d) details of the steps the reporting PSP or IPSP has taken.

53. The obligation in the second subparagraph of point (2) of Article 8 of Regulation (EU) 2015/847 applies without prejudice to the obligation to report suspicious transactions pursuant to Article 33 of Directive (EU) 2015/849.

54. PSPs and IPSPs should notify relevant authorities upon identifying a repeatedly failing PSP or IPSP without undue delay, and no later than three months after identifying the repeatedly failing PSP or IPSP.

55. These authorities will then notify the EBA.

Steps to be taken

56. The steps the PSP of the payee or the IPSP should 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.

57. 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 in line with Article 19 of Directive (EU) 2015/849.

CHAPTER III: Additional obligations for the IPSP

58. 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, IPSPs should satisfy themselves of their system's ability to convert information into a different format without error or omission.

59. 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.[4] 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. Such alternative mechanisms should be used only during a short transition period while domestic systems are being adjusted to comply with Regulation (EU) 2015/847 and these guidelines.

[4] Article 10 of Regulation (EU) 2015/847.

CHAPTER IV: Additional obligations for the PSP of the payee

Incomplete information

60. PSPs of the payee should follow the guidance in Chapter II of these guidelines also in relation to information that is incomplete.

Verification of information on the payee

61. When verifying the accuracy of information on the payee pursuant to points (3) and (4) of Article 7 of Regulation (EU) 2015/847, PSPs should consider whether or not their relationship with the payee amounts to a business relationship as defined in point (13) of Article 3 of Directive (EU) 2015/849 and apply customer due diligence measures in line with point (1) of Article 13 of Directive (EU) 2015/849 should that be the case.

62. PSPs may consider that they have complied with the verification requirements in Article 7 of Regulation (EU) 2015/847 where they have previously verified the payee's identity in line with the national law transposing point (1)(a) of Article 13 and, where applicable, point (1)(b) of Article 13 of Directive (EU) 2015/849 or to an equivalent standard, should the payee's identity have been verified before the legislation transposing Directive (EU) 2015/849 entered into force.

Record-keeping

63. 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 that Regulation.

64. However, where the PSP has entered into a business relationship with the payee and the transfer of funds takes place in the context of that business relationship, PSPs should comply with the record-keeping requirements in Article 40 of Directive (EU) 2015/849.

Title III — Final provisions and implementation

65. Competent authorities and PSPs should comply with these guidelines six months from their date of issue.

Annex — 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.	

*For further information and guidance, please refer to the European Supervisory Authorities' 'Joint guidelines under Article 25 of Regulation (EU) 2015/847 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'.