JC/GL/2017/16

05/04/2017

Consultation Paper

Draft 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

Contents

1. Responding to this consultation

The European Supervisory Authorities (the ESAs) invite comments on all proposals put forward in this paper and in particular on the specific questions summarised in section 5.2.

Comments are most helpful if they:

- respond to the question stated;
- indicate the specific point to which a comment relates;
- contain a clear rationale;
- provide evidence to support the views expressed/ rationale proposed; and
- describe any alternative regulatory choices the ESAs should consider.

Submission of responses

To submit your comments, click on the 'send your comments' button on the consultation page by 5 June 2017. Please note that comments submitted after this deadline, or submitted via other means may not be processed.

Publication of responses

Please clearly indicate in the consultation form if you wish your comments to be disclosed or to be treated as confidential. A confidential response may be requested from us in accordance with the ESAs' rules on public access to documents. We may consult you if we receive such a request. Any decision we make not to disclose the response is reviewable by the ESAs' Board of Appeal and the European Ombudsman.

Data protection

The protection of individuals with regard to the processing of personal data by the ESAs is based on Regulation (EC) N° 45/2001 of the European Parliament and of the Council of 18 December 2000 as implemented by the ESAs in their implementing rules adopted by their Management Boards. Further information on data protection can be found under the Legal notice section of the ESAs' website.

2. Executive Summary

On 26 June 2015, Regulation (EU) 2015/847 on information accompanying transfers of funds (Regulation (EU) 2015/847) entered into force. This Regulation aims, inter alia, to bring European legislation in line with Recommendation 16 of the International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation that the Financial Action Task Force (FATF), an international anti-money laundering standard setter, adopted in 2012.

In line with the FATF's Recommendation 16, Regulation (EU) 2015/847 specifies which information on the payer and the payee payment service providers (PSPs) have to attach to funds transfers. It also requires PSPs to put in place effective procedures to detect transfers of funds that lack this information, and to determine whether to execute, reject or suspend such transfers of funds. The objective is to prevent the abuse of fund transfers for terrorist financing and other financial crime purposes, to detect such abuse should it occur, to support the implementation of restrictive measures and to allow relevant authorities to access the information promptly.

However, Regulation (EU) 2015/847 does not set out in detail what PSPs should do to comply. Article 25 of Regulation (EU) 2015/847 therefore requires the European Supervisory Authorities (ESAs) to issue guidelines to competent authorities and PSPs on the measures PSPs should take to comply with Regulation (EU) 2015/847 and in particular in relation to the implementation of Articles 7, 8, 11 and 12 of that Regulation.

Through these guidelines, the ESAs aim to promote the development of a common understanding, by PSPs and competent authorities across the EU, of what effective procedures to detect and manage transfers of funds that lack required information on the payer and the payee are, and how they should be applied. A common understanding is essential to ensure the consistent application of EU law; it is also conducive to a stronger European anti-money laundering and countering the financing of terrorism (AML/CFT) regime.

3. Background and rationale

On 26 June 2015, Regulation (EU) 2015/847 on information accompanying transfers of funds entered into force and is applicable from 26 June 2017. This Regulation aims to bring European legislation in line with Recommendation 16 of the International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation that the Financial Action Task Force (FATF), an international anti-money laundering standard setter, adopted in 2012.

In line with the FATF's Recommendation 16, Regulation (EU) 2015/847 aims to make the abuse of funds transfers for terrorist financing and other financial crime purposes more difficult and to enable relevant authorities fully to trace such transfers where this is necessary to prevent, detect or investigate money laundering or terrorist financing (ML/TF).

To this end, Regulation (EU) 2015/847:

- lays down rules on the information on the payer and the payee that must accompany a transfer of funds, in any currency, where at least one of the Payment Service Providers (PSPs) in the payment chain is established in the Union;

- requires the PSP of the payee and the intermediary PSP to put in place effective procedures to detect transfers of funds that lack required information on the payer and the payee; and

- requires the PSP of the payee and the intermediary PSP to put in place effective risk-based procedures to determine whether to execute, reject or suspend a transfer of funds that lacks required information on the payer or the payee, and which follow up action to take.

However, Regulation (EU) 2015/847 does not set out in detail what PSPs should do to comply. Article 25 of Regulation (EU) 2015/847 therefore requires the European Supervisory Authorities (ESAs) to issue guidelines to competent authorities and PSPs on the measures PSPs should take to comply with Regulation (EU) 2015/847 and in particular in relation to the implementation of Articles 7, 8, 11 and 12 of that Regulation.

These guidelines:

- help PSPs determine which transfers of funds are within the scope of Regulation (EU) 2015/847, including with regard to the exemptions foreseen in Article 2(3) of the Regulation;

- help PSPs determine which role they play in the payment chain and consequently, which obligations Regulation (EU) 2015/847 imposes on them. This is important, because Regulation (EU) 2015/847 does not require intermediary PSPs to identify whether

information on the payer or the payee that accompanies a transfer of funds is incomplete.

- provide PSPs 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;

- set out the risk factors PSPs 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 the lack of information gives rise to suspicion of ML/TF; and

- help competent authorities assess whether the procedures PSPs have put in place to comply with Articles 7, 8, 11 and 12 of Regulation (EU) 2015/847 are adequate and effective.

These guidelines focus on measures to comply with articles 7, 8, 11 and 12 of Regulation (EU) 2015/847, but similar considerations apply in relation to articles 9 and 13 of Regulation (EU) 2015/847.

They guidelines build on the *Common Understanding of the obligations imposed by European Regulation 1781/2006 on the information on the payer accompanying funds transfers to payment service providers of payees* the ESAs' predecessors CEBS, CESR and CEIOPs adopted in October 2008.[1] However, their scope is wider and takes account of the new legal framework and international AML/CFT standards that have since emerged.

Annexes I to III set out which information on the payer and the payee must accompany a transfer of funds.

[1]CEBS 2008 156/ CEIOPS-3L3-12-08/ CESR/08-773 (2008): Common understanding of the obligations imposed by European Regulation 1781/2006 on the information on the payer accompanying funds transfers to payment service providers of payees http://www.eba.europa.eu/-/the-three-level-3-committees-publish-today-their-common-understanding-in-relation-to-the-information-on-the-payer-of-accompanying-fund-transfers-to-pa

4. 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 dd.mm.yyyy (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).

Title I - Subject matter, scope and definitions

Subject matter and scope

1. These guidelines are addressed to

    - Payment Service Providers (PSPs) defined in Article 3(5) and Article 3(6) of Regulation (EU) 2015/847; and

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

2. These guidelines

    - set out the factors PSPs 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

    - specify what PSPs 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 to comply with Articles 7, 8, 11 and 12 of Regulation (EU) 2015/847.

4. PSPs 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 and PSPs should consider other factors and measures as appropriate.

6. Compliance with 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') is outside the scope of these guidelines.

Definitions

7. For the purpose of these Guidelines, the following definitions shall apply:

    - 'Competent authorities' means the authorities responsible for ensuring PSPs' compliance with the requirements of Regulation (EU) 2015/847.

- 'Receiving PSP' means the PSP receiving the transfer. This can be either an intermediary PSP or the PSP of the payee.

- 'Sending PSP' means the PSP sending the transfer and can be either the PSP of the payer or the last intermediary PSP in the payment chain.

- 'Risk' means the impact and likelihood of ML/TF taking place.

- '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.

- 'Risk based approach' means an approach whereby competent authorities and PSPs identify, assess and understand the ML/TF risks to which PSPs are exposed and take AML/CFT measures that are proportionate to those risks.

- 'Meaningless information' means information that makes no obvious sense such as strings of random characters (e.g. 'xxxxx', or 'ABCDEFG') or clearly meaningless designations (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.

- 'Missing information' means a blank field or meaningless information.

- 'Incomplete information' means information on the payer or the payee that is only partially provided, for example an initial rather than a first name, or a country without the postal address.

- 'Real-time monitoring' refers to monitoring performed

    - 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, before the funds are made available to the payee by the PSP who receives the funds; or

    - Where the PSP is an intermediary PSP, before the intermediary PSP transfers the funds on behalf of the PSP of the payer or of another intermediary PSP.

- '*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, after the funds have been made available to the payee by the PSP (for the PSP of the payee) or transmitted (for the intermediary PSP); or

- where the PSP is an intermediary PSP, after the intermediary PSP has transferred the funds on behalf of the PSP of the payer or of another intermediary PSP.

Title II- Requirements regarding the measures taken by PSPs in the detection of missing information and the transfers of fund without this information

CHAPTER I: General considerations

Establishing the PSP's obligations under Regulation (EU) 2015/847

8. PSPs should assess in which capacity they intervene in the payment chain because this will determine which information is required and what they have to do to comply with Regulation (EU) 2015/847.

9. As part of this, PSPs should consider whether they act on behalf of the payer, on behalf of the payee, or merely intervene on behalf of another PSP:

    - The PSP acting on behalf of the payer is the one responsible for ordering the transfer of funds and should always be considered the PSP of the payer.

    - The PSP acting on behalf of the payee is the one responsible for accepting the transfer of funds and should always be considered the PSP of the payee.

10. To benefit from the derogation in Article 5 of Regulation (EU) 2015/847, PSPs should be able to determine whether a PSP in the chain is based in a third country, outside the EU/EEA.

Benefiting from exemptions from Regulation (EU) 2015/847

11. PSPs must comply with Regulation (EU) 2015/847 in respect of all transfers of funds that are made electronically and irrespective of the messaging or payment and settlement system used, unless they can benefit from exemptions in Article 2 of Regulation (EU) 2015/847 apply.

12. To benefit from these exemptions, PSPs should have in place systems and controls to ensure the conditions for these exemptions are met.

Linked transactions

13. To benefit from exemptions for transfers of funds that do not exceed EUR 1000, PSPs should put in place systems and controls to detect transactions that appear to be linked. Linked transaction are at least those transactions that are being sent

    - from the same payments account or the same payer to the same payee; and

- within a short time-frame, for example within six months;

Proportionality and business-wide risk assessments

14. PSPs should establish and maintain effective policies and procedures to comply with Regulation (EU) 2015/847 that are proportionate to the nature and size of the PSP and commensurate to the ML/TF risk to which the PSP is exposed as a result of:

    - the type of customers it attracts and the nature of the persons it services;
    - the nature of the products and services it provides;
    - the jurisdictions it services;
    - the delivery channels it uses;
    - the number of PSPs regularly failing to provide required information on the payer and the payee;
    - the complexity of the payment chains in which it intervenes, as a result of its business model; and
    - the volume and the size of transactions it processes.

15. When assessing the ML/TF risk to which they are exposed, PSPs should refer to the ESAs' 'Joint Guidelines 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'.

Policies and procedures

16. PSPs should ensure that their policies and procedures :

    - enable them effectively to comply with Regulation (EU) 2015/847, taking into account the ML/TF risk to which they are exposed. For example, exclusively manual transaction monitoring should be used only where this does not hamper the PSP's ability effectively to check and process the volume of transactions it receives.

    - set out clearly
        - which criteria the PSP will use to determine whether the PSP's services and payment instruments fall under the scope of Regulation (EU) 2015/847, and which services and payment instruments will always be within the scope of Regulation (EU) 2015/847;

  - which transfers have to be monitored in real-time, and which can be monitored ex-post, and why;
  - what staff should do where required information is missing (and, where appropriate, their respective responsibilities); and
  - which information has to be recorded, how it should be recorded, and where.

- are approved by their senior management, as defined by Directive (EU) 2015/847;

- are available to all persons responsible for ensuring the PSP's compliance with Regulation (EU) 2015/847 and that all persons responsible for ensuring the PSP's compliance with Regulation (EU) 2015/847 are appropriately trained in the application of these policies and procedures; and

- are reviewed regularly, improved where necessary and kept up to date.

Use of existing systems and controls to comply with Regulation (EU) 2015/847

17. To the extent possible, PSPs may use existing systems and controls, such as systems to detect where transactions may involve individuals and organisations subject to financial sanctions, to detect incomplete or missing required information in accordance with Regulation (EU) 2015/847.

CHAPTER II: Obligations on intermediary PSPs and PSPs of the payee

Detection of inadmissible characters or inputs (Article 7(1) and Article 11(1) of Regulation (EU) 2015/847)

19. PSPs should monitor transfers of funds in real time to detect whether 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 effect the transfer.[2]

20. A PSP may assume that it complies with Article 7(1) and Article 11(1) of Regulation (EU) 2015/847 if it is satisfied, and can demonstrate, to its competent authority, that it understands which characters or inputs comply with the conventions of the messaging, or payment and settlement system it uses, and that it understands the system's validation rules. The PSP should be satisfied that its system:

    - Contains all the fields necessary to obtain the information required by Regulation (EU) 2015/847. For SEPA and intra-Union transactions, this includes the account number or IBAN of the payer and the payee or a unique transaction identifier;

    - Automatically prevents the sending or receiving of payments should inadmissible characters or inputs be detected; and

    - Flags rejected payments for manual review and processing.

21. Should a PSP have doubts about the system meeting these criteria, it should put in place controls to mitigate the shortcomings identified.

Detection of missing information on the payer or the payee (Articles 7(2) and 11(2) of Regulation (EU) 2015/847

22. PSPs must implement effective procedures to detect whether the required information on the payer or the payee is missing.[3]

23. PSPs should treat obviously meaningless information as though it was missing information.

24. Effective procedures should include a combination ex-post and real-time monitoring. PSP should refer to the risk factors in paragraph 14 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 they are exposed to as a business.

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

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

25. High risk transfers of funds should be monitored in real time. Therefore, where PSPs do not routinely monitor transactions in real time, they should configure their systems in a way that alerts them to high risk indicators that may trigger real-time monitoring. These include, but are not limited to,

    - transfers of funds that exceed a certain (high) value. When deciding on the threshold, PSPs 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;

    - transfers of funds where the payer or the payee are based in a country associated with high ML/TF risk; and

    - transfers of funds from a PSP that the PSP knows has repeatedly failed to provide required information on the payer without good reason (see paragraphs 45-50).

26. Ex-post monitoring should include both random sampling and targeted sampling, in line with a risk-based approach.

27. When choosing samples for risk-based, targeted ex-post monitoring, PSPs should pay particular attention to transfers of funds meeting the criteria in paragraph 25 as well as:

    - PSPs that have been identified as presenting a higher ML/TF risk;

    - PSPs that have previously been known to fail to provide required information on the payer of the payee, even if they did not repeatedly fail to do so;

    - Transfers where the name of the payer or the payee are missing.

Actions to be taken to manage transfers of funds with missing information on the payer or the payee, or inadmissible characters or inputs

28. PSPs 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.

29. In those cases, PSPs should consider the risk of ML/TF associated with the individual funds transfer before deciding on the appropriate course of action, and in particular whether:

    - the type of information missing gives rise to concern;

    - the transfer is from a high risk third country;

    - there are other indicators that suggest that the transaction presents a high ML/TF risk or gives rise to suspicion of ML/TF.

a. The PSP chooses to reject the transfer

30. Where a PSP chooses to reject a transfer, it does not have to ask for missing information but should share the reason for the rejection with the sending PSP.

b. The PSP suspends the transfer

31. Where a PSP chooses to suspend the transfer of funds, it should ask the sending PSP to supply the information on the payer or the payee that is missing, or to provide that information using admissible characters or inputs.

32. When asking for missing information, the PSP should set a reasonable timeframe, within which the sending PSP should answer. The timeframe should be set out in the PSP's procedures. This should not exceed 3 working days for intra-EEA transfers, and 5 working days for transfers of funds from outside the EEA. The PSP should notify the sending PSP that the transfer has been suspended.

33. PSPs should consider sending a reminder to the sending PSP should the requested information not be forthcoming. As part of this, PSPs may decide to warn the sending PSP that in case no satisfactory answer is received within the deadline, the sending PSP will be subject to the internal high risk monitoring (see paragraph 25) and treated as 'repeatedly failing' as set out in Article 8(2) of Regulation 2015/847.

34. Where the requested information is not forthcoming within the timeframe set by the PSP, the PSP should, in line with its risk-based policies and procedures, decide whether to reject or execute the transfer, consider whether the PSP's failure to supply the requested information gives rise to suspicion and consider the future treatment of the sending PSP for AML/CFT compliance purposes.

35. The PSP 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, in particular where as a result of actions taken under Article 8 of Regulation (EU) 2015/847, the PSP has been unable to comply with relevant obligations in Articles 83 and 84 of Directive (EU) 2015/2366 as transposed into the applicable national legal framework.

c. The PSP executes the transfer

36. Where a PSP chooses to execute the transfer of funds, or detects ex-post that information was missing or provided using inadmissible characters, it should ask the sending PSP to supply 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.

37. PSPs who become aware of missing information while carrying out real-time monitoring should document their reason for executing the transfer.

38. When asking for missing information, the PSP should set a reasonable timeframe, within which the sending PSP should respond. The timeframe should be set out in the PSP's

procedures. This should not usually exceed 3 working days for intra-EEA transfers, and 5 working days for transfers of funds from outside the EEA.

39. PSPs should consider sending a reminder to the sending PSP should the requested information not be forthcoming. As part of this, PSPs may decide to warn the sending PSP that in case no satisfactory answer is received within the deadline, the sending PSP will be subject to the internal high risk monitoring (see paragraph 25) and treated as 'repeatedly failing' as set out in Article 8(2) of Regulation 2015/847.

40. Where the requested information is not forthcoming within the timeframe set by the PSP, the PSP should, in line with its risk-based policies and procedures, consider whether the PSP's failure to supply the requested information gives rise to suspicion and consider the future treatment of the sending PSP for AML/CFT compliance purposes.

41. The PSP 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.

Reporting and assessment (Articles 9 and 13)

42. To comply with Articles 9 and 13 of Regulation (EU) 2015/847, PSPs should assess whether a transfer is suspicious based on criteria set out in national law and their own, internal AML/CFT policies and procedures. PSPs should note that missing or inadmissible information may not, by itself, give rise to suspicion of ML/TF; when considering whether a transfer of funds raises suspicion, the PSP should instead take a holistic view of all ML/TF risk factors associated with the transfer of funds, including those listed in Paragraph 25, to the extent that these are known.

43. PSPs should pay particular attention to transactions that are likely to present a higher risk of ML/FT such as transfer of funds from countries identified as high risk by the European Commission in accordance with Article 9 of the Directive (EU) 2015/849.

44. PSPs must at all times comply with national legislation, including in cases where this requires them to take additional action, for example the reporting of unusual transactions that may not give rise to suspicion .

PSPs that are repeatedly failing to provide the required information and steps to be taken (Articles 8.2 and 12.2)

What is 'repeatedly failing' to provide required information

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

46. To this end, PSPs should keep a record of all transactions with missing information, including the sending PSP, the amount and the type of missing information of each one of the cases, to be able to determine which PSP should be classified as 'repeatedly failing'.

47. A PSP may decide to treat PSPs as 'repeatedly failing' for different reasons, which may include either, or a combination of, quantitative and qualitative criteria.

48. Examples of quantitative criteria for assessing whether a PSP is repeatedly failing include :

- the percentage of transfers with missing information sent by a specific PSP within a certain timeframe; and
- the percentage of follow-up requests that were left unanswered or were not adequately answered within a certain timeframe.

49. Examples of qualitative criteria for assessing whether a PSP is repeatedly failing include:

- the level of cooperation of the requested PSP relating to previous requests for information; and
- the type of information missing.

50. PSPs may consider tightening the criteria for sending PSPs that are associated with a high ML/TF risk.

Notifying the authorities

51. Once a PSP has identified another PSP as repeatedly failing to provide the required information in line with paragraphs 45-50, the PSP must within one calendar month or earlier if required by national law, inform the authorities specified in Article 8(2) of Regulation (EU) 2015/847 who will then notify the European Banking Authority.

52. This report should include at least:

- the name of the PSP identified as repeatedly failing to provide the required information;
- the country in which the PSP is authorised;
- the nature of the breach, including the frequency of transfers with missing information, the period of time for which the breaches were identified and any reasons the PSP may have given to justify their repeated failure to provide the required information; and
- details of the steps the reporting PSP has taken.

53. This obligation to inform competent authorities of PSPs that repeatedly fails to provide the required information applies without prejudice to obligations of suspicious transaction reporting pursuant to Article 33 of the Directive (EU) 2015/849.

Steps to be taken

54. Where a PSP repeatedly fails to provide information required by Regulation (EU) 2015/847, the PSP of the payee must take steps to address this.[4] These steps should be risk-based.

55. As a first step, the receiving PSP should issue a warning to the sending PSP to inform the PSP of the steps that will be applied should the PSP continue to fail to provide the information required by Regulation (EU) 2015/847.

56. PSPs should further consider how the repeated failure by the PSP to provide information and the PSP's attitude to responding to such requests affects the ML/TF risk associated with the PSP, and where appropriate, carry out real-time monitoring of all transactions received from that PSP.

57. Should the sending PSP continue to fail to provide the required information, the PSP should issue a second warning to the sending PSP that it will reject any future transfers of funds. As a last step, this may lead to the PSP restricting or terminating its business relationship.

58. Before taking the decision to terminate a business relationship, in particular where the sending PSP is a respondent bank from a third country, the PSP should consider whether 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.

[4] Articles 8(2) and 12(2) of Regulation (EU) 2015/847

CHAPTER III: Additional obligation for the intermediary PSP

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

60. PSPs should only use payment or messaging systems that permit the onward transfer of all information on the payer or the payee, irrespective of whether this information is required by Regulation (EU) 2015/847.[5]

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

CHAPTER IV: Additional obligations for the PSP of the payee

Incomplete information

61. PSPs of the payee should follow the guidance in Chapter II.2 and II.3 of these guidelines also in relation to information that is incomplete.

Verification of information on the payee

62. The PSP of the payee must verify the accuracy of information on the payee where

    - the transfer of funds exceeds EUR 1000 in one single transaction, or linked transactions; or
    - the payee receives the funds in cash; or
    - The payee receives the funds as electronic money and the PSP is not satisfied that the payee's identity will have been verified by the electronic money issuer; or
    - The PSP of the payee has reasonable grounds to suspect ML/TF.[6]

63. In those cases, the PSP should apply the same risk-sensitive verification standards as they would apply to comply with Article 13 (1)(a) and, where applicable, Article 13(1)(b) of Directive (EU) 2015/849 as transposed by national legislation.

64. PSPs should consider whether their relationship with the payee amounts to a business relationship as defined in Article 3(13) of Directive (EU) 2015/849 and apply customer due diligence measures in line with Article 13(1) of Directive (EU) 2015/849 should that be the case.

65. 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 Article 13 (1)(a) and, where applicable, Article 13(1)(b) 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. [7]

[6] Article 7 (3) and Article 7(4) of Regulation (EU) 2015/847

[7] Article 7(5) of Regulation (EU) 2015/847

Title III- Final Provisions and Implementation

67. Competent authorities should implement these guidelines by incorporating them into their supervisory processes and procedures by [xxx].

Annex 1 – Required information: obligations on the payment service provider of the payer

Obligations on the PSP of the payer														
Location of the other PSPs		Ammount		Required information (articles 4 and 5, with derrogations laid down in Article 6)							Obligation to verify the information on the payer		
						On the payer			On the payee				
Intermediary PSPs (if any)	PSP of the payee	Exceeding €1000*	Not exceeding €1000**	To be provided together with the transfer***	To be provided at the request of the PSP of the payee or the intermediary PSP [article 5(2)]	Name	Payment account number or unique transaction identifier	Address or official personal document number or customer identification number or date and place of birth	Name	Payment account number or unique transaction identifier	Always	When there are ML/TF suspicions	Funds received in cash or in anonymous e-money
Established within or outside the EU	Established outside the EU	X		X		X	X	X	X	X	X		
			X	X		X	X		X	X		X	X
Established within or outside the EU	Established within the EU	X		X			X			X	X		
					X	X	X	X	X	X	X****		
			X	X			X			X	X		
					X	X	X		X	X		X****	X****

* Whether the concerned transfers are carried out in a single transaction or in several transactions which appear to be linked

** If the concerned transfers do not appear to be linked to other transfers of funds which, together with the transfer in question, exceed EUR 1 000

*** Without prejudice to batch file transfers, in which case the information provided is in respect of that batch file

**** Information initially provided on the payer together with the transfer of funds has to be verified before the execution of that transfer. Where further requests are made under Article 5(2), the PSP may assume that the information initially provided has already been verified when changes to that information are not deemed to have taken place

Annex 2 – Required information: obligations on the payment service provider of the payee

Obligations on the PSP of the payee													
Location of the other PSPs		Ammount of the transfer		Required information (articles 4 and 5, with derrogations laid down in Article 6)								Obligation to verify the information on the payee	
						On the payer			On the payee				
PSP of the payer	Intermediary PSPs (if any)	Exceeding €1000*	Not exceeding €1000**	To be provided together with the transfer***	To be provided at the request of the PSP of the payee or the intermediary PSP [article 5(2)]	Name	Payment account number or unique transaction identifier	Address or official personal document number or customer identification number or date and place of birth	Name	Payment account number or unique transaction identifier			
Established within the EU	Established within or outside the EU	X		X			X			X		Always****	
					X	X	X	X	X	X			
			X	X			X			X			When there are ML/TF suspicions or the pay-out is made in cash or in anonymous e-money****
					X	X	X		X	X			
Established outside the EU	Established within or outside the EU	X	X	X		X	X	X	X	X		Always, if the transfer of funds **exceeds €1000***	When there are ML/TF suspicions or the pay-out is made in cash or in anonymous e-money, if the transfer **does not exceed €1000****

* Whether the concerned transfers are carried out in a single transaction or in several transactions which appear to be linked
** If the concerned transfers do not appear to be linked to other transfers of funds which, together with the transfer in question, exceed EUR 1 000
*** Without prejudice to batch file transfers, in which case the information provided is in respect of that batch file
**** Information initially provided on the payee together with the transfer of funds has to be verified before crediting the payee's payment account or making the funds available to the payee. Where further requests are made under Article 5(2), the PSP may assume that the information initially provided (payee's payment account number or unique transaction identifier) has already been verified when changes to that information are not deemed to have taken place

Annex 3 – Required information: obligations on the intermediary payment service provider

Obligations on intermediary PSPs										
Location of the other PSPs		Ammount				Required information (articles 4 and 5, with derrogations laid down in Article 6)				
						On the payer			On the payee	
PSP of the payer	PSP of the payee	Exceeding €1000*	Not exceeding €1000**	To be provided together with the transfer***	To be provided at the request of the PSP of the payee or the intermediary PSP [article 5(2)]	Name	Payment account number or unique transaction identifier	Address or official personal document number or customer identification number or date and place of birth	Name	Payment account number or unique transaction identifier
Established within the EU	Established outside the EU	X		X		X	X	X	X	X
			X	X		X	X		X	X
Established within the EU	Established within the EU	X		X			X			X
					X	X	X	X	X	X
			X	X			X			X
					X	X	X		X	X
Established outside the EU	Established within or outside the EU	X		X		X	X	X	X	X

* Whether the concerned transfers are carried out in a single transaction or in several transactions which appear to be linked
** If the concerned transfers do not appear to be linked to other transfers of funds which, together with the transfer in question, exceed EUR 1 000
*** Without prejudice to batch file transfers, in which case the information provided is in respect of that batch file

5. Accompanying documents

5.1 Draft impact assessment

Article 25 of Regulation (EU) 2015/847 requires the European Supervisory Authorities (ESAs) to issue Guidelines to competent authorities and payment service providers (PSPs) on 'the measures to be taken in accordance with this Regulation, in particular as regards the implementation of Articles 7, 8, 11 and 12'.

This document provides an overview of the issues identified, the options considered and the potential impact of these options on PSPs and national competent authorities.

A. Problem identification

Tracking financial flows can be an important tool in the prevention, detection and investigation of terrorist financing and other financial crimes.[8] Regulation (EU) 2015/847 therefore sets out which information on the payer and the payee must accompany a transfer of funds. It also requires PSPs to put in place effective systems and controls to detect transfers of funds that lack required information, and risk-based policies and procedures to determine whether to execute, reject or suspend a transfer of funds that lacks the required information. However, Regulation (EU) 2015/847 does not set out in detail what PSPs must do to comply. There is, therefore, a possibility that PSPs and competent authorities interpret and apply these Regulations inconsistently, leaving the Union's financial market exposed to the risk of monetary laundering and terrorist financing (ML/TF).

B. Policy objectives

Through these Guidelines, the ESAs aim to promote the development of a common understanding, by PSPs and competent authorities across the EU, of effective procedures to detect and manage transfers of funds that lack the information on the payer or the payee required by Regulation (EU) 2015/847. A common understanding is essential to ensure the consistent interpretation and application of Union law and conducive to a stronger European anti-money laundering and countering the financing of terrorism (AML/CFT) regime.

As part of this, the joint Guidelines should not only set clear regulatory expectations, but at the same time leave sufficient room for PSPs to define their approach in a way that is proportionate to the nature and size of their business and commensurate with the ML/TF risk they are exposed to.

[8] European Commission (2016): Action plan to strengthen the fight against terrorist financing, February 2016.

C. Baseline scenario

In October 2008, the ESAs' predecessors published a 'Common understanding of the obligations imposed by European Regulation 1781/2006 on the information on the payer accompanying funds transfers to payment service providers of payees'. This Common Understanding determines how PSPs and competent authorities interpret their obligations under Regulation (EC) 1781/2006, which preceded Regulation (EU) 2015/847. While many of the Common Understanding's conclusions remain important, the scope and underlying legal basis have changed to reflect revised international standards and best practice. Furthermore, the Common Understanding did not compel financial institutions and competent authorities to 'comply or explain'.[9]

In the baseline scenario the implementation of Regulation (EU) 2015/847 takes effect without accompanying ESAs' Guidelines, but with a non-binding Common Understanding that addresses some, but not all, aspects of Regulation (EU) 2015/847.

D. Options considered

In drafting these Guidelines, the ESAs considered the views of AML/CFT competent authorities and informal feedback from private sector stakeholders. Different options on the scope of the mandate and the approach of the Guidelines have been identified, and their costs and benefits assessed for their ability to achieve the ESAs' policy objectives.

1. Scope of the mandate

The ESAs' mandate in Article 25 of Regulation (EU) 2015/847 requires the ESAs to issue Guidelines on the implementation of Articles 7, 8, 11 and 12 of Regulation (EU) 2015/847, but does not limit the Guidelines to these articles.

Option 1.1: The ESAs could extend the scope of the mandate to draft Guidelines on all aspects of Regulation (EU) 2015/847. This would include Guidelines for PSPs of the payer.

Option 1.2: The ESAs could focus on the articles listed in the mandate, but touch upon related issues in other articles where this is necessary to ensure the consistent application of the Regulation's obligations. Or,

Option 1.3: The ESAs could write Guidelines exclusively on the articles listed in their mandate.

[9] Article 16(3) of Regulation (EU) No 1093/2010.

2. Approach

The ESAs' mandate in Article 25 of Regulation (EU) 2015/847 requires the joint Guidelines to be targeted and proportionate, however it does not prescribe the approach the ESAs should take. While Regulation (EU) 2015/847 forms part of the Union's wider AML/CFT framework, which is risk-based, the Regulation contains a number of provisions that are prescriptive and leave PSPs and competent authorities little room for manoeuvre.

Option 2.1: The Guidelines could be detailed and prescriptive with a view to achieving maximum harmonisation of PSPs' approaches to complying with Regulation (EU) 2015/847;

Option 2.2: The Guidelines could provide enough detail to enable PSPs to identify areas of high risk and focus their efforts to comply with Regulation (EU) 2015/847 on those areas, but leave it to PSPs to decide how best to comply; and,

Option 2.3: The Guidelines could prescribe what PSPs should do in certain situations, whilst allowing PSPs some flexibility to accommodate different risk scenarios.

E. Cost-Benefit Analysis and preferred options

The implementation of the different options would create both benefits and costs for PSPs and competent authorities. All options the ESAs have considered create one-off costs for PSPs to review and adapt existing systems and controls, and ongoing costs for PSPs and competent authorities to train staff in the application and assessment of these systems and controls. These costs derive mainly from changes to the Union's legal framework. However, the joint Guidelines allow PSPs to build on systems established under the Common Understanding, which can limit the costs for some PSPs that already apply the principles set out in the Common Understanding and for the supervision of these systems by competent authorities.

1. Scope

Before this background, the main advantage of Option 1.1 would be that comprehensive Guidelines on all aspects of Regulation (EU) 2015/847 would increase regulatory certainty and create a more harmonised European approach to providing information with transfers of funds. Although arguably more costly than other options, Option 1.1 could be conducive to a more effective European funds transfer regime going forward, as national differences would be kept to a minimum. The main disadvantage associated with Option 1.1 is that it would leave little room for adjustment, and give rise to the risk of the Guidelines' systems and controls provisions being disproportionate for at least some PSPs.

The main advantage of Option 1.2 would be that greater regulatory certainty would be achieved in key areas where this is necessary to achieve a consistent and effective pan-European approach. Examples of areas that would benefit from additional Guidelines include the identification and reporting of suspicious transaction reports, and the requirement for intermediaries to retain all

information with the transfer of funds. The disadvantage of Option 1.2 is that under this Option PSPs could incur greater one-off costs to review and update their systems and controls in light of new expectations than under the baseline scenario or Option 1.3.

The main advantage of Option 1.3 is that Guidelines that focus exclusively on the articles listed in Article 25 of Regulation 2015/847 are conducive to achieving consistency where the legislator felt this was necessary, without creating additional compliance costs. Furthermore, some of the issues where Option 1.2 might introduce greater consistency could be addressed at least in part through other Guidelines, for example under Articles 17 and 18(4) of Directive (EU) 2015/849. Option 1.3 is therefore likely to be more targeted than Options 1.1 and Option 1.2. However, certain provisions in Regulation (EU) 2015/847 are not sufficiently clear and are not addressed in other supranational Guidelines, and could therefore be interpreted differently by competent authorities and PSPs in different Member States.

Option 1.2 is the retained option. The benefits associated with greater regulatory certainty and consistency of approach that can be expected from Guidelines on issues beyond those described in Articles 7, 8, 11 and 12 of Regulation (EU) 2015/847, are expected to outweigh the additional compliance burden for PSPs. When implementing the additional requirements PSPs can leverage on their measures necessary to comply with the requirements in Article 7, 8, 11 and 12. Option 1.2 reduces the risk of creating regulatory arbitrage and reduces compliance costs for PSPs that operate across borders and whose approach may otherwise be deemed inadequate by other competent authority. It further assures a more harmonised European approach for providing payer information on transfers of funds which is tailored to the areas of highest need and a more effective fight against terrorist financing in particular.

2. Approach

The main advantage of Option 2.1 is that detailed and prescriptive Guidelines would reduce uncertainty and create maximum harmonisation of practices. Some industry representatives suggested that this might be desirable. However, initial set-up costs are likely to be high as PSPs would have to adjust their systems to match the new requirements, and on-going compliance costs might increase for PSPs whose size or business models might be better suited to alternative systems and controls. For competent authorities, Option 2.1 would facilitate the assessment of PSPs' systems and controls to comply with Regulation (EU) 2015/847 as prescriptive Guidelines could reduce the need for specialist supervisors trained to exercise informed judgement.

The advantage of Option 2.2 is that it would allow PSPs to identify and focus on those areas where the risk of ML/TF associated with transfers of funds is highest. This approach would allow PSPs to adopt the approach that is best suited to their particular nature and size – for example, some PSPs that are not credit institutions have suggested that one size does not fit all. However, Option 2.2 would not achieve the same degree of regulatory certainty as Option 2.1 and could create costs by distorting competition, as PSPs and competent authorities in different Member States could interpret the same provisions unevenly. PSPs in Member States that have not had a tradition of the

risk-based approach to AML/CFT might also incur additional costs to employ or train staff competent for assessing and managing ML/TF risk. For competent authorities, Option 2.2 would create the highest costs as the assessment of diverse approaches to comply with Regulation (EU) 2015/847 can be complex and requires supervisors to have access to experts able to exert sound judgement on the adequacy of PSPs' systems and controls.

The advantage of Option 2.3 is that it sets clear expectations in cases where this is necessary and proportionate, for example in relation to checking whether information contained in a transfer of funds is missing or obviously meaningless, while at the same time allowing PSPs to make risk-based decisions on the most appropriate and effective way to comply with Regulation (EU) 2015/847 where the size and nature of PSPs' business might justify different approaches. For PSPs, Option 2.3 might create some one-off costs to adjust their systems and controls and costs to employ or train staff in the application of the risk-based approach, where this approach is new. For competent authorities, the same considerations apply as in Option 2.2, whereas the costs are mitigated in the cases in which PSPs are restricted to a prescriptive approach.

Option 2.3 is the retained option. It combines the benefits of non-standardised approaches for PSPs and of a prescriptive approach for competent authorities. PSPs will benefit from gbeing able to tailor their risk identification and management systems and controls to their own risk profile. For competent authorities, the benefits of this approach are that it will help supervisors set clear expectations of the factors PSPs should consider when detecting and management missing payer information on financial transfers, while at the same time mitigating costs by building on existing regulatory guidance to PSPs and supervisory manuals. Option 2.3 supports the ESAs' objective to draft proportionate and effective Guidelines on identifying transfers of funds with missing or incomplete information and taking appropriate follow up action because they are conducive to a common approach in those areas where consistency and regulatory certainty is needed, while at the same time allowing PSPs some flexibility in the way they design and implement the systems and controls to comply with Regulation (EU) 2015/847.

Overall, the benefits from these Guidelines are expected to outweigh potential costs and these Guidelines are expected contribute to making the fight against terrorist financing and money laundering more effective.

5.2 Questions for consultation

Q1: Do you agree with the general considerations in Chapter 1? In particular, do you agree that these are necessary to ensure an effective, risk-based and proportionate approach to complying with Regulation (EU) 2015/847?

If you do not agree, clearly set out your rationale and provide supporting evidence where available. Please also set out what you consider to be the common principles that apply to both, the PSP of the payee and the intermediary PSP, and why.

Q2: Do you agree that the expectations on intermediary PSPs and PSPs of the payee in Chapter II are proportionate and necessary to both comply with Regulation (EU) 2015/847 and ensure a level playing field?

In particular, do you agree with:

- The steps PSPs should take to detect and manage transfers of funds with missing information of inadmissible characters or inputs?
- The steps PSPs should take to detect and manage PSPs that are repeatedly failing to provide the required information?

If you do not agree, clearly set out your rationale and provide supporting evidence where available. Please also set out at what you believe PSPs should do instead, and why.

Q3: Do you agree with the provisions for intermediary PSPs in Chapter III?

If you do not agree, clearly set out your rationale and provide supporting evidence where available. Please also set out how you think intermediary PSPs can meet their obligations in Article 10 of Regulation (EU) 2015/847 instead.

Q4: Do you agree with the provisions for PSPs of the payee in Chapter IV?

If you do not agree, clearly set out your rationale and provide supporting evidence where available. Please also set out how you think PSPs of the payee can meet their obligations instead.