



JOINT COMMITTEE OF THE EUROPEAN
SUPERVISORY AUTHORITIES

JC 2017 08

10/02/2017

Consultation Paper

On

Joint draft Regulatory Technical Standards on the criteria for determining the circumstances in which the appointment of a central contact point pursuant to Article 45(9) of Directive (EU) 2015/849 is appropriate and the functions of the central contact point

Contents

1. Responding to this Consultation	3
2. Executive Summary	4
3. Background and rationale	5
4. Joint Regulatory Technical Standards	9
5. Accompanying documents	16
5.1 Impact Assessment	16
5.2 Overview of questions for the public consultation	27

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 May 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

Payment service providers and electronic money issuers with a head office in an EU Member State can operate establishments in other, host, Member States. Such establishments have to comply with the anti-money laundering and countering the financing of terrorism (AML/CFT) regime of the Member State in which they are based, even if they are not obliged entities themselves.

To facilitate the AML/CFT supervision of such establishments, several Member States require payment service providers and electronic money issuers to appoint a 'Central Contact Point' (CCP). A CCP acts as a point of contact between the payment service provider or electronic money issuer and the host Member State's competent authority. However, in the absence of a common European approach to CCPs, there is a risk of regulatory arbitrage, which threatens to undermine the robustness of Europe's AML/CFT defenses. There is also a risk that legal uncertainty creates unreasonable obstacles for payment service providers and electronic money issuers wishing to provide their services on a cross-border basis.

Article 45(10) of Directive (EU) 2015/849 therefore requires the European Supervisory Authorities (ESAs) to draft Regulatory Technical Standards (RTS). These draft RTS

- Create legal certainty about the criteria Member States will use to determine whether a CCP must be appointed; and
- Clearly set out the functions a CCP must have to fulfil its duties.

In line with the mandate in Article 45(10), these draft RTS do not specify the form a CCP must take or determine when payment service providers or electronic money issuers provide services in another Member State through establishments.

Next Steps

The ESAs will finalise these draft RTS once the public consultation has closed. They will then submit the final draft to the European Commission for approval.

3. Background and rationale

On 26 June 2015, Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (Directive (EU) 2015/849) entered into force. This Directive aims, inter alia, to bring European legislation in line with 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 and counter-terrorist financing standard setter, adopted in 2012.

In line with the FATF's standards, Directive (EU) 2015/849 puts the risk-based approach at the centre of the European Union's anti-money laundering (AML) and counter-terrorist financing (CFT) regime. It recognises that the risk of money laundering (ML) and terrorist financing (TF) can vary and that Member States, competent authorities and obliged entities have to take steps to identify and assess that risk with a view to deciding how best to manage it.

Credit and financial institutions that are within the scope of Directive (EU) 2015/849 have to comply with the AML/CFT regime of the Member State in which they are established. This means that payment service providers and electronic money issuers ('institutions') that operate an establishment other than a branch in another Member State will have to ensure that this establishment complies with the host Member State's AML/CFT requirements.¹ An 'establishment other than a branch' can include agents of payment service providers² and persons distributing electronic money on the electronic money issuer's behalf³.

Directive 2005/60/EC made clear that branches of credit or financial institutions that are located in another Member State are obliged entities. It did not address the phenomenon of establishments other than a branch, like agents of payment service providers or electronic money distributors. Notwithstanding, the territorial approach in Directive 2005/60/EC meant that those establishments were nevertheless expected to comply with the host Member State's AML/CFT requirements, whether or not they were themselves obliged entities. This created challenges for competent authorities of host Member States in supervising those establishments' compliance with local AML/CFT requirements.

As a result, some Member States required institutions that were headquartered in another European Member State but provided services in their jurisdiction through agents and, in some cases, distributors, to appoint 'central contact points'. These central contact points serve as a point of contact between the host competent authority and the institution situated in another Member State, which facilitates the AML/CFT supervision of agent and distributor networks in the

¹ Article 45(2) of Directive (EU) 2015/849

² Article 4(38) of Directive (EU) 2015/2366 defines 'agent' as 'a natural or legal person who acts on behalf of a payment institution in providing payment services'

³ Directive 2009/110/EC

host Member State's territory. The Commission's proposal for a Fourth Anti-Money Laundering Directive, which was published in 2013, suggested that the European Supervisory Authorities (ESAs) should develop draft Regulatory Technical Standards to ensure that Member States that require institutions to appoint a Central Contact Point adopt a consistent approach and to make sure that this requirement is proportionate to the money laundering and terrorist financing risk.

Article 45(10) of Directive (EU) 2015/849 - Application and scope

Article 45(10) of Directive (EU) 2015/849 requires the ESAs to draft Regulatory Technical Standards on the criteria Member States should use when deciding whether foreign institutions that operate establishments other than a branch on the Member State's territory should appoint a Central Contact Point and what the functions of that Central Contact point should be. The ESAs have to submit these draft Regulatory Technical Standards to the Commission by 26 June 2017.

The requirements set out in the draft Regulatory Technical Standards will apply where

- a) Member States decide to require Central Contact Points. Where Member States do not to require institutions to appoint Central Contact Points, these draft Regulatory Technical Standards will not apply; and
- b) Institutions that have their head office in another Member State operate establishments other than a branch on the host Member State's territory. A CCP is not required where institutions do not operate establishments, because they make use of the free provision of services.

Article 45(10) of Directive (EU) 2015/849 does not authorise the ESAs to determine when agents or persons distributing electronic money on an electronic money issuer's behalf are establishments.

The mandate does not extend either to determining the form a Central Contact Point should take. Consequently, any decision about who the Central Contact Point should be and how it has to be set up will be the host Member State's.

Criteria

These draft Regulatory Technical Standards set out a two-pronged approach to deciding whether the appointment of a Central Contact Point is appropriate

Host Member States can require institutions that are headquartered in another Member State to appoint a Central Contact Point if certain quantitative criteria are met, namely:

- c) The number of establishments other than a branch that the institution operates on the host Member State's territory is, or exceeds, ten; or
- d) the amount of the electronic money distributed and redeemed, or the value of the payment transactions executed by such establishments is expected to exceed EUR 3 million per financial year or has exceeded EUR 3 million in the previous financial year; or
- e) the information necessary to assess whether criterion (a) or (b) is met is not made available to the host Member State's competent authority upon request and in a timely manner.

Host Member States can also require institutions that are headquartered in another Member State to appoint a Central Contact point if the money laundering or terrorist financing risk associated with the operation of these institutions' establishments other than a branch is such that the appointment of a Central Contact Point is proportionate even if the criteria in a), b) or c) are not met.

The intention is to create legal certainty and a consistent interpretation of the Central Contact Point provisions across the EU, whilst at the same time allowing Member States to require the Central Contact Points where this is necessary in light of, and commensurate to, the money laundering and terrorist financing risk associated with the operation of foreign institutions' establishments on their territory.

Functions

Article 45(9) of Directive (EU) 2015/849 is clear that a Central Contact Point has two main functions:

- a) To ensure, on the appointing institution's behalf, compliance with the host Member State's AML/CFT requirements and
- b) To facilitate supervision by the host Member State's competent authorities. This includes providing the host Member State's competent authorities with documents and information upon request.

This means that central contact points will need to, at a minimum, inform the appointing institution of applicable AML/CFT rules and how these might affect the institution's AML/CFT policies and processes; oversee the compliance by establishments other than a branch with applicable AML/CFT rules and take corrective action where necessary.

As part of this, central contact points also need to, at a minimum, be able to access information held by establishments other than a branch; represent the appointing institution in

communications with the Member State's competent authorities and the FIU; and facilitate on-site inspections of establishments if necessary.

Whilst not explicitly required, this implies that the central contact point should have adequate technical knowledge of applicable AML/CFT requirements as well as sufficient human and financial resources to carry out their functions.

Member States may also determine, based on their assessment of money laundering and terrorist financing risk, that as part of their duty to ensure compliance with local AML/CFT obligations, the central contact points be required to perform certain additional functions. In particular, it may be appropriate for Member States to require the central contact point to submit suspicious transaction reports to the host FIU.

Failure to comply

Article 48(4) of Directive (EU) 2015/849 makes clear that competent authorities of the host Member State must supervise that foreign payment service providers and electronic money issuers who operate establishments other than a branch on their territory comply with their AML/CFT obligations. This may include taking temporary measures to address serious failings by those establishments, provided that the nature of the failing means that taking immediate corrective action is necessary.

The power of host competent authorities to sanction breaches of institutions' establishments on their territory is outside the scope of the mandate in Article 45(10) of Directive (EU) 2015/849.

Central Contact Point provisions in Directive (EU) 2015/2366

Article 29(5) of Directive (EU) 2015/2366 requires the European Banking Authority (EBA) to draft Regulatory Technical Standards, which set out criteria for the appointment of Central Contact Points of payment service providers and their functions to ensure the protection of consumers in the Member State in which a payment service provider operates establishments other than a branch. The purpose of these central contact points is different from that foreseen under Directive (EU) 2015/849.

4. Joint Regulatory Technical Standards

COMMISSION DELEGATED REGULATION (EU) No .../..

of **XXX**

[...]

supplementing Directive (EU) 2015/849 of the European Parliament and of the Council with regard to regulatory technical standards on the criteria for determining the circumstances in which the appointment of a central contact point for electronic money issuers and payment service providers is appropriate pursuant to Article 45(9) and the functions of such central contact points

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC⁴, and in particular Article 45(10),

Whereas:

- (1) Member States may require the appointment of a Central Contact Point where the size and scale of the activities carried out by payment service providers and electronic money issuers through establishments in forms other than a branch meets or exceeds certain thresholds. These thresholds should be set at a level that is proportionate to the aim of the Directive to facilitate supervision by competent authorities of such establishments' compliance, on their appointing institution's behalf, with local anti-money laundering and countering the financing of terrorism (AML/CFT) obligations, while at the same time not creating undue regulatory burden on payment service providers and electronic money issuers.

⁴

OJ L 141, 5.6.2015, p.73.

- (2) The requirement to appoint a central contact point may also be justified where a Member State considers that the risk of money laundering and terrorist financing associated with the operation of such establishments is increased, as demonstrated, for instance, on the basis of an assessment of the money laundering and terrorist financing (ML/TF) risk associated with certain categories of payment service providers or electronic money issuers. Member States should not be required to risk assess individual institution for that purpose.
- (3) However, in exceptional cases, where Member States have reasonable grounds to believe that the ML/TF risk associated with a particular payment service provider or electronic money issuer that operates establishments on their territory is high, they should be able to require that institution to appoint a central contact point even if it does not meet the thresholds or belong to a category of institutions that is required to appoint a central contact point based on the Member State's assessment of ML/TF risk.
- (4) Where a central contact point is appointed, it should ensure, on behalf of the appointing institution, the compliance of the establishments of the appointing institution with the applicable AML/CFT rules. To this end, the central contact point should have a sound understanding of applicable AML/CFT requirements and facilitate the development and implementation of AML/CFT policies and procedures.
- (5) The central contact point should, amongst others, have a central coordinating role between the appointing institution and its establishments on the one hand, and the appointing institution and the competent authorities of the Member State where the establishments operate on the other hand, to facilitate their supervision.
- (6) Member States may determine, based on their overall assessment of money laundering and terrorist financing risk associated with the activity of payment service providers and electronic money issuers that are established on their territory in forms other than a branch, that as part of their duty to ensure compliance with local AML/CFT obligations, central contact points be required to perform certain additional functions. In particular, it may be appropriate for Member States to require central contact points to submit, on behalf of the appointing institution, suspicious transaction reports to the FIU of the Member State in whose territory the obliged entity is established.
- (7) This Regulation is based on the draft regulatory technical standards submitted by the European Supervisory Authorities (European Banking Authority, European Insurance and Occupational Pensions Authority, European Securities and Markets Authority) to the Commission.
- (8) The European Supervisory Authorities have conducted open public consultations on the draft regulatory technical standards on which this Regulation is based, analysed the potential related costs and benefits and requested the opinion of the Banking Stakeholder Group established in accordance with Article 37 of

Regulation (EU) No 1093/2010⁵, Regulation (EU) No 1094/2010⁶ and Regulation (EU) No 1095/2010⁷ respectively.

HAS ADOPTED THIS REGULATION:

Article 1- Subject matter and scope

This Regulation lays down rules concerning:

- a) criteria for determining the circumstances in which the appointment of a central contact point pursuant to Article 45(9) of Directive (EU) 2015/849 is appropriate;
- b) the functions of such central contact points.

Article 2 –Definitions

For the purposes of this Regulation, the following definition shall apply:

- (1) ‘competent authority’ means the authority competent for ensuring compliance of electronic money issuers and payment service providers that are established on their territory in forms other than a branch and whose head office is situated in another Member State with the requirements of Directive (EU) 2015/849 as transposed by national legislation;
- (2) ‘host Member State’ means the Member State on whose territory electronic money issuers and payment service providers whose head office is situated in another Member State are established in forms other than a branch;
- (3) ‘institution’ means electronic money issuers as defined in point (3) of Article 2 of Directive 2009/110/EC⁸ and payment services providers as defined in point (9) of Article 4 of Directive 2007/64/EC⁹.

⁵ 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 (OJ L 331, 15.12.2010, p. 12).

⁶ Regulation (EU) No 1094/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Insurance and Occupational Pensions Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/79/EC (OJ L 331, 15.12.2010, p.48).

⁷ Regulation (EU) No 1095/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Securities and Markets Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/77/EC (OJ L 331, 15.12.2010, p. 84).

⁸ Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC (OJ L 267, 10.10.2009, p.7).

⁹ Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC (OJ L 319, 5.12.2007, p.1).

Section 1

Circumstances in which the appointment of a central contact point is appropriate

1. **Article 3 – Criteria** Host Member States may require institutions that are established on their territory in forms other than a branch, and whose head office is situated in another Member State, to appoint a central contact point if any of the following conditions are met:
 - (a) the number of such establishments, is equal to, or exceeds, ten; or
 - (b) the amount of the electronic money distributed and redeemed, or the value of the payment transactions executed by such establishments is expected to exceed EUR 3 million per financial year or has exceeded EUR 3 million in the previous financial year; or
 - (c) the information necessary to assess whether criterion (a) or (b) is met is not made available to the host Member State's competent authority upon request and in a timely manner.
2. Without prejudice to the conditions set out in paragraph 1, host Member States may require categories of institutions that are established on their territory in forms other than a branch and whose head office is situated in another Member State to appoint a central contact point in situations where this is commensurate to the level of money laundering or terrorist financing risk associated with the operation of those institutions' establishments.

Host Member States shall base their assessment of the level of money laundering or terrorist financing risk associated with the operation of such establishments on the findings of risk assessments carried out in accordance with Article 6(1) and Article 7(1) of Directive (EU) 2015/849 and other credible and reliable sources available to them. As part of this, host Member States shall take into account at least:

- (a) the money laundering and terrorist financing risk associated with the types of products and services offered and the distribution channels used;
- (b) the money laundering and terrorist financing risk associated with the types of customers;
- (c) the money laundering and terrorist financing risk associated with the prevalence of occasional transactions over business relationships; and
- (d) the money laundering and terrorist financing risk associated with the countries and geographic areas serviced.

3. Without prejudice to the conditions set out in paragraph 1 and 2, host Member State may in exceptional cases empower the host Member State's competent authority to require an institution that is established in its territory in forms other than a branch and whose head office is situated in another Member State to appoint a central contract point providing that the- host Member State or the host Member State's competent authority has reasonable grounds to believe that the operation of establishments of that institution presents a high money laundering and terrorist financing risk. .

Section 2

Functions of the central contact points

Article 4 – Assurance of compliance with AML/CFT rules

A central contact point shall ensure that establishments specified in Article 45(9) of Directive (EU) 2015/849 comply with AML/CFT rules of the host Member State. To this end, a central contact point shall:

- (a) facilitate the development and implementation of AML/CFT policies and procedures pursuant to Article 8(3) and (4) of Directive EC 2015/849;
- (b) oversee, on behalf of the appointing institution, the effective compliance by such institution's establishments, with applicable AML/CFT requirements and the appointing institution's policies controls and procedures adopted pursuant to Article 8(3) and (4) of Directive (EU) 2015/849;
- (c) inform the head office of the appointing institution of any breaches or compliance issues encountered in such establishments, including any information that might affect the establishment's ability to comply effectively with the appointing institution's AML/CFT policies and procedures or may otherwise affect the appointing institution's risk assessment;
- (d) take, on behalf of the appointing institution, corrective action, in case of non-compliance or risk of non-compliance by such establishments with applicable AML/CFT rules;
- (e) ensure that such establishments and their staff participate in training programmes referred to in Article 46(1) of Directive (EU) 2015/849; and
- (f) represent the appointing institution in its communications with the competent authorities and the FIU of the host Member State.

Article 5 – Facilitation of supervision by competent authorities of the host Member State

A central contact point shall facilitate supervision by competent authorities of the host Member State of establishments specified in Article 45(9) of Directive (EU) 2015/849. To this end, a central contact point shall, on behalf of the appointing institution:

- (a) represent the appointing institution in its communications with competent authorities;
- (b) access information held by such establishments;
- (c) respond to any request made by competent authorities related to the activity of such establishments, and provide relevant information related to such establishments to competent authorities. Where appropriate, reporting shall be done on a regular basis; and
- (d) facilitate on-site inspections of such institution's establishments if required by the competent authorities.

Article 6– Additional functions of a central contact point

1. In addition to the functions specified in Articles 4 and 5 host Member States may require central contact points to perform one or more of the following functions:
 - (a) filing reports pursuant to Article 33(1) of Directive (EU) 2015/849 as transposed in national law of the host Member State;
 - (b) responding, on behalf of the appointing institution, to any request of the FIU related to the activity of establishments specified in Article 45(9) of Directive (EU) 2015/849, and providing relevant information related to such establishments to the FIU;
 - (c) scrutinising transactions to identify suspicious transactions.
2. Host Member States may oblige central contact points to perform one or more of the additional functions specified in paragraph 1 where this is commensurate to the overall level of money laundering and terrorist financing risk associated with the operation of those payment service providers and electronic money issuers that are established on their territory in forms other than a branch.

Host Member States shall base their assessment of the level of money laundering or terrorist financing risk associated with the operation of such establishments on the findings of risk assessments carried out in accordance with Article 6(1) and Article 7(1) of Directive (EU) 2015/849, Article 3(2) of this Regulation where applicable and other credible and reliable sources available to them.

Article 7

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels,

*For the Commission
The President*

*[For the Commission
On behalf of the President*

[Position]

5. Accompanying documents

5.1 Impact Assessment

1. Article 45(10) of Directive (EU) 2015/849 requires the European Supervisory Authorities (ESAs) to draft Regulatory Technical Standards (RTS) on the criteria Member States should apply to determine whether payment service providers or electronic money issuers that are established on their territory in forms other than a branch and whose head office is situated in another Member State must appoint a Central Contact Point (CCP), and what the functions of that CCP will be.
2. This document considers advantages and disadvantages of different policy options and assesses the impact the preferred options will have on payment service providers, electronic money issuers and competent authorities.

A. Problem identification and baseline scenario

3. Directive (EU) 2015/849 aims to bring European legislation in line with 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 Standards, Directive (EU) 2015/849 recognises that the risk of money laundering and terrorist financing (ML/TF) can vary and that Member States, competent authorities and obliged entities have to take steps to identify and assess that risk with a view to deciding how best to manage it.
4. Obligated entities are subject to the anti-money laundering and counter-terrorist financing (AML/CTF) regime of the Member State in which they are based. This means that credit and financial institutions that operate an establishment in another (host) Member State will have to ensure that this establishment complies with the host Member State's AML/CTF requirements. The establishment will be supervised for compliance with these requirements by the host competent authority.¹⁰
5. This approach can be challenging where institutions provide services in another member state through agents or persons who distribute electronic money on the electronic money issuer's behalf. Article 45(9) of Directive (EU) 2015/849 therefore envisages the creation of 'Central Contact Points', that serve as a point of contact between a host supervisor and

¹⁰ Article 48(4) of Directive (EU) 2015/849

a payment institution or electronic money issuer from another Member State and facilitate the AML/CFT supervision of networks of agents or persons distributing electronic money where applicable.

6. Article 45(10) of Directive (EU) 2015/849 requires the ESAs to draft RTS on the criteria to be used when deciding whether foreign payment service providers or electronic money issuers that operate establishments on the host Member State's territory should appoint a 'Central Contact Point' and what the functions of that Central Contact Point should be. In the absence of such RTS, there will be no consistent approach to the appointment and functions of a CCP in the EU and a resultant risk of regulatory arbitrage, as well as legal uncertainty for payment service providers and electronic money issuers wishing to provide their services on a cross-border basis. This is the baseline scenario.

B. Policy Objectives

7. In drafting these RTS, the ESAs' overall policy objective is to foster the adoption of a coherent and risk-based approach across the EU in the areas specified in Article 45(10) of Directive (EU) 2015/849, and to do so in a way that is both proportionate and effective and does not unreasonably create obstacles to the operation of establishments other than a branch on a host Member State's territory.
8. Specifically,
 - with regard to the appointment of a CCP, the ESAs' aim is to create greater legal certainty about the criteria Member States will use to determine whether this is necessary and commensurate to the ML/TF risk; and
 - with regards to the functions a CCP should have, the ESAs' aim is to be clear about what CCPs must be able to do to ensure, on the appointing institution's behalf, compliance with the host Member State's AML/CFT requirements and to facilitate supervision of compliance with those requirements by the host Member State's competent authorities;

9. Article 45(10) of Directive (EU) 2015/849 does not give the ESAs a mandate to draft RTS on the form a CCP should have, nor to determine when agents or distributors may be establishments.

C. Options considered and preferred options

10. The ESAs considered the views expressed by AML/CFT competent authorities in two questionnaires and subsequent discussions and informal feedback from private sector stakeholders as well as other quantitative and qualitative data the ESAs had at their disposal.

C.1. Criteria Member States shall use to determine when a CCP is required

11. Article 45(10) of Directive (EU) 2015/849 mandates the ESAs to set out which criteria Member States should use to determine whether the appointment of a CCP is appropriate.
12. European legislation is clear that a CCP is not required where payment service providers or electronic money issuers do not operate establishments because they make use of the free provision of services.
13. This means that the first criterion host Member States have to consider is whether the payment service provider or electronic money issuer operates an establishment other than a branch on its territory. However, establishing criteria for determining when an agent or distributor becomes an establishment is outside the scope of these draft RTS.
14. The second criterion host Member States have to consider is whether the appointment of a CCP is proportionate.
15. There are a number of policy options.
 - (ii) All foreign payment service providers or electronic money issuers that operate establishments in a host Member State have to appoint a CCP (Option 1.1)
16. The RTS could allow Member States to require the appointment of a CCP wherever a foreign payment service provider or electronic money issuer operates one or more establishments in the host Member State.
17. The advantage of this option is that it could provide for a harmonised approach to CCPs and a level playing field across the EU.
18. The disadvantage of this option is that this requirement is unlikely to be proportionate, as it fails to take into account the ML/TF risk associated with the establishment's operation and the practicalities associated with the AML/CFT supervision of such establishments by the host Member State's competent authority.
 - (iii) A CCP is required where a foreign payment service provider or electronic money issuer operates ten or more establishments in the host Member State (Option 1.2).
19. Directive (EU) 2015/849 envisages that the appointment of a CCP will facilitate the AML/CTF supervision of a foreign payment service provider's or electronic money issuer's establishments by the host Member State's competent authority. The number of establishments that triggers a CCP requirement should therefore reflect the point at which it becomes difficult for the host competent authority effectively to supervise compliance with local AML/CFT requirements.

20. Feedback from competent authorities suggests that this point is reached where the number of establishments of a foreign payment service provider or electronic money issuer in the host Member State is, or exceeds, ten.

21. The advantage of this option is that it creates regulatory certainty as it establishes a definitive quantitative threshold. It is also proportionate, as the majority of payment service providers and electronic money issuers do not operate more than five establishments on another Member State's territory (though a small number of payment service providers operate more than 100 establishments in some Member States).

22. The disadvantages are that:

- a) the number of establishments alone does not take into account transaction volumes or ML/TF risk associated with the nature and type of the product or service provided;
 - b) there is a risk that institutions might structure their foreign operations in a way that the quantitative requirement is not met;
 - c) Member States may come to different conclusions when determining whether one agent or person distributing electronic money on an electronic money issuer's behalf is a legal entity (e.g. supermarket chain XYZ) or the number of operational parts of that legal entity (e.g. each of supermarket chain XYZ's branches); and
 - d) in the absence of clear legal obligations on foreign payment service providers or electronic money issuers, or home competent authorities, to make available the information required for the assessment of the quantitative thresholds, the host competent authority may be unable to assess whether these thresholds are met.
- (iv) A CCP is required where a foreign payment service provider or electronic money issuer transacts, or distributes and redeems, more than three million EUR per financial year through their establishments in the host Member State (Option 1.3).

23. Under this option, the RTS set a monetary threshold for both the amount of electronic money distributed and redeemed, and the amount of payment transactions executed. A CCP will be required where either threshold is reached or exceeded. This threshold should be set at a level where the operation of the institution's establishments on the host MS's territory is deemed complex, which means that the risk of ML/TF is unlikely to be low. Once this threshold has been reached or exceeded, a CCP will be required.

24. Feedback from competent authorities suggests that this threshold should be set at three million EUR.

25. The advantage of this Option is that it creates regulatory certainty as it establishes a definitive quantitative threshold. It is also proportionate since it takes into account the size of the activities of the agent or distributor network and captures those business

models that involve relatively few but high value or high risk transactions; establishments providing few, lower risk products and services only are unlikely to be caught. Member States that already require the appointment of CCPs report that based on their experience, this level is also proportionate to the cost associated with the establishment and running of a CCP.¹¹

26. The disadvantages are the following:

- a) Monthly or annual figures can be volatile and fluctuate significantly;
 - b) Differences in purchasing power in different Member States are not taken into account;
 - c) Higher transaction amounts or turnover may not necessarily be an indicator of ML/TF risk;
 - d) in the absence of clear legal obligations on foreign payment service providers or electronic money issuers, or home competent authorities, to make available the information required for the assessment of the quantitative thresholds, the host competent authority may be unable to assess whether these thresholds are met; and;
 - e) a monetary threshold set at this level might act as a barrier to market entry in some cases where a Member State's requirements on the form a CCP must take offer little flexibility
- (v) A CCP is required where the Member State assesses that the operation of establishments other than a branch increases the money laundering or terrorist financing risk (Option 1.4).

27. Under this option, the RTS would set out which criteria the host Member State must consider when determining whether the establishment of agents or persons distributing electronic money on an electronic money issuer's behalf increases the ML/TF risk in the host Member State's territory.

28. The advantage of this option is that this is in line with the risk-based approach required by Directive (EU) 2015/849. The appointment of a Central Contact Point will be proportionate to the ML/TF risk posed by the establishment of agents or persons distributing electronic money on an electronic money issuer's behalf, or networks of agents or distributors. It is also cost-effective, as Member States will be able to draw on their national ML/TF risk assessments and the Commission's supranational risk assessment. There is no expectation that Member States carry out individual risk assessments of each payment service provider, electronic money issuer, agent, person

¹¹ The cost of establishing and running a CCP will be determined by the form a CCP is required to take. The ESAs' mandate does not extend to determining what that form might be.

distributing electronic money on an electronic money issuer's behalf, or networks thereof. Nevertheless, in exceptional cases, where a Member State has reasonable grounds to believe that the ML/TF risk associated with the operation of a specific payment service provider's or electronic money issuer's establishments on the Member State's territory is high, it would be able to require that payment service provider or electronic money issuer to appoint a CCP.

29. The disadvantage is that this approach may not create a level playing field because the decision whether to require the appointment of a CCP will ultimately be the Member State's, based on their assessment of the ML/TF risk. This criterion, by itself, also fails to acknowledge practical difficulties associated with the AML/CTF supervision of large numbers of establishments.

(vi) a CCP is required where either the number of establishments exceeds a certain threshold or the value of payment transactions or electronic money distribution and redemption in the host's territory exceeds EUR 3 million per calendar year or the Member State assesses that the operation of establishments other than a branch increases the ML/TF risk (Option 1.5).

30. This option is a combination of Options 1.2, 1.3 and 1.4. In this option, a drawback linked to the availability of information to support the assessment of quantitative thresholds under Options 1.2 and 1.3 is mitigated by including an additional criterion on access to information, which makes clear that it will be in an institution's interest to make this information available upon request: should relevant information not be forthcoming, this will be grounds for the appointment of a CCP.

31. The advantage of this option is that it is in line with the risk-based approach in Directive (EU) 2015/849 and conducive to a proportionate outcome. It also creates regulatory certainty as it includes a quantitative threshold above which a CCP is always required and makes it more difficult for institutions to avoid specific quantitative thresholds.

32. The disadvantage is that Member States may come to a different view of the extent to which the outcome of their assessment of ML/TF risk justifies the appointment of CCPs where the quantitative criteria are not met, which means that differences in the Union may remain.

Preferred option

33. Option 1.5 is the preferred option as it combines quantitative criteria with a more qualitative risk assessment. It sets a definitive quantitative threshold across all Member States, which is related to the number of establishments on the host Member State's territory and a monetary threshold that reflects the nature and complexities of the services provided. At the same time, it allows Member States to require the appointment of CCPs where this is commensurate to the ML/TF risk.

C.2 CCP functions

34. Article 45(10) of Directive (EU) 2015/849 mandates the ESAs to set out which functions a CCP should have. These fall into two broad categories:

- To ensure compliance, on behalf of the appointing institution, with applicable AML/CTF rules and
- To facilitate supervision by competent authorities, including by providing competent authorities with documents and information on request.

35. The ESAs consider that to ensure compliance, a CCP will need to, at least:

- Oversee the effective implementation, by establishments, of AML/CTF policies and procedures on the payment service provider's or electronic money issuer's behalf and take corrective action where necessary either on the payment service provider's or electronic money issuer's behalf or by informing the payment service provider or electronic money issuer of any breaches or compliance issues encountered;
- Have adequate financial, human and technical resources to perform their functions;
- Have a sound knowledge of applicable AML/CTF requirements; and,
- Inform the development of AML/CTF policies, controls and procedures in line with Article 8(3) and (4) of Directive (EU) 2015/849 and training in line with Article 46 of Directive (EU) 2015/849.

36. To facilitate supervision, a CCP will need to, at least:

- Have the ability to access information held by local establishments;
- Have the ability to respond to any question, and provide relevant information on the payment service provider or electronic money issuer's behalf to the host AML/CTF competent authority, including, where appropriate, on a regular basis;
- Represent the payment service provider or electronic money issuer in communications with the host AML/CTF competent authority; and,
- Facilitate on-site inspections of local establishments if required by the host AML/CTF competent authority.

37. With this in mind, the RTS could set out:

- (i) a definitive list of functions that all CCPs must be able to perform (Option 2.1)

38. The RTS could set out a definitive list of functions all CCPs must perform in line with those set out in paragraphs 35 and 36. Member States would not be able to require CCPs to perform additional functions.

39. The advantage of this option is that it sets out clearly which functions a CCP must always have to meet the overarching objective in Article 45(9) of Directive (EU) 2015/849. It is conducive to maximum harmonisation and legal certainty.

40. The disadvantage is that setting out a definitive list of functions does not take into account specific circumstances, such as a Member State's legal and regulatory framework or the need to address particular ML/TF risks that have been identified at the national level, where additional functions will be necessary to ensure that CCPs can effectively comply with their obligations under Article 45(9) of Directive (EU) 2015/849. This might stand in the way of the effective implementation of Article 45(9) of Directive (EU) 2015/849.

(ii) a list of core functions, which can be complemented with additional functions (Option 2.2)

41. The RTS could set out a definitive list of functions all CCPs must perform but give Member States the option of requiring the CCP to perform additional functions subject to certain criteria.

42. This option recognises that there may be specific circumstances where the imposition of additional functions on CCPs may be appropriate to ensure that CCPs can effectively ensure compliance with local AML/CFT obligations. In particular, it may be appropriate for Member States to require the central contact point to facilitate interactions with the host Financial Intelligence Unit (FIU). Such additional functions would consist of:

- submitting suspicious transaction reports to the local FIU;
- Responding, on behalf of the appointing institution, to any request related to the activity of establishments and provide relevant information upon request;
- Representing the payment service provider or electronic money issuer in communications with the host Member State's FIU;
- Scrutinising transactions to identify suspicious transactions.

43. The advantages of this approach are that it accommodates differences in Member States' legal system and approach to AML/CFT, while at the same time preserving a minimum common standard. It is also compatible with the AMLD's principle that the appointing institution is ultimately responsible for their establishments' failure to comply with applicable AML/CFT obligations, and in line with the Directive's risk-based approach.

44. The disadvantage is that this approach introduces an element of uncertainty for payment service providers and electronic money issuers, as Member States' practices can differ on this particular point.

(iii) a list of core functions with the possibility of waivers (Option 2.3)

45. The RTS could set out a comprehensive list of functions a CCP must perform but give Member States the option of waiving one or several functions in cases where the ML/TF risk associated with an institution's establishments other than a branch justifies this. The advantage of this option is that it would help ensure that the CCP requirement is proportionate and can be tailored to specific risk scenarios.

46. However, responses from competent authorities to a cost-benefit questionnaire suggest that the cost associated with the introduction of waivers is greater for both competent authorities that have to consider waiver requests and institutions that have to apply for these, than a set list of functions.

47. Furthermore, the introduction of waivers leads to a loss of legal certainty for institutions and may not be compatible with the maximum harmonisation mandate the ESAs have under Article 48(10) of Directive (EU) 2015/849.

Preferred option

48. Option 2.2 is the preferred option because it ensures both a level playing field by requiring a core list of key functions while at the same time recognising that additional functions may be necessary to ensure that the appointment of a CCP meets the objective of Article 45(9) of Directive (EU) 2015/849.

D. Impact assessment

49. The implementation of the ESAs' preferred options will create costs and benefits for both, competent authorities and payment service providers and electronic money issuers.

50. One-off costs for competent authorities will arise from the need to obtain the information necessary to assess whether the criteria for the appointment of a CCP are met. However, the ESAs' preferred option frames those criteria in a way that those costs are unlikely to be significant: competent authorities will be able to draw on existing data, such as passporting notifications and their Member State's national risk assessments under Article 6 of Directive (EU) 2015/849, to inform their analysis. There is no expectation that the Member States carry out individual risk assessments of each agent, person distributing electronic money on an EMI behalf, or networks thereof.

51. Where Member States do not already operate a CCP regime, or have to amend an existing regime in light of these RTS, competent authorities will also face one-off costs to set up a suitable regime for ensuring CCP oversight.
52. Ongoing costs for competent authorities will arise from the need to ensure effective AML/CFT oversight. This cost exists already, independently from these RTS, and depends on the nature and size of the sector in each Member State. However, competent authorities from Member States that already have a CCP requirement indicated that the cost of supervision of CCPs was unlikely to exceed 2 FTE; and some competent authorities from Member States that did not already require a CCP expected their ongoing cost of supervision to reduce. No competent authority expected the cost of supervision to rise as a result of introducing a CCP requirement.
53. For competent authorities, the preferred options therefore lead to a net benefit in the medium term. This is because information from Member States' competent authorities that already require the appointment of CCPs suggests that the benefits associated with the appointment of a CCP, such as easier access to information to facilitate supervision and a single point of contact between the host authority and the appointing institution, are greater than the costs to competent authorities arising from an assessment whether a CCP is warranted.
54. The preferred options will create both one-off and ongoing costs for payment service providers and electronic money issuers that operate establishments other than a branch in another Member State, provided that these establishments meet the criteria for the appointment of a CCP and that the host Member State opts to require CCPs.
55. The costs related to the setting up and operation of a CCP will be determined by the form a CCP will take and depend at least in part on the particular circumstances of a host Member State, such as the cost of labour or (where applicable) the cost of office space. The ESAs' mandate in Article 45(10) of Directive (EU) 2015/849 does not extend to determining the form a CCP should take and any decision about who the CCP should be and how it should be set up is the host Member State's. Nevertheless, the functions envisaged by the ESAs' preferred option suggest that all CCPs will have to have some human and financial resources adequately to carry out their functions.
56. Information from competent authorities in Member States that already require CCPs suggests that these costs are unlikely to act as a barrier to market entry and do not impose additional cost burden on providers other than those required in any case to comply with the local AML/CFT regime. Competent authorities from Member States that already require the appointment of CCPs report a significant increase in the number of agents and persons distributing electronic money on an electronic money issuers behalf, and a public consultation in one Member State on the requirement to appoint a CCP yielded no negative responses. Furthermore, greater consistency in the way CCPs are appointed and the functions a CCP must have will benefit those payment service

providers and electronic money issuers that provide services through establishments other than a branch in other Member States.

57. In the medium to long term, the ESAs expect the net impact of the ESAs' preferred options on payment service providers and electronic money issuers to be insignificant, though the extent to which costs will outweigh the expected benefits will depend on external factors outside of the ESAs' mandate, such as the form the CCP will take and labour market conditions in the host Member State.

5.2 Overview of questions for the public consultation

Q1: Do you agree with the criteria for a requirement to appoint a Central Contact Point (CCP)?
In particular,

- do you agree that it is proportionate to require the appointment of a CCP where
 - the number of establishments is equal to, or exceeds, ten; or
 - the amount of electronic money distributed and redeemed, or the value of the payment transactions executed by such establishments is expected to exceed EUR 3 million per financial year or has exceeded EUR 3 million in the previous financial year?

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

- do you agree that Member States should be able to
 - require all institutions, or certain categories of institutions, to appoint a CCP where this is commensurate with the ML/TF risk associated with the operation of these institutions' establishments on the Member State's territory; and
 - empower competent authorities to require an institution to appoint a CCP where they have reasonable grounds to believe that the establishments of that institution present a high money laundering and terrorist financing risk, even if the criteria in Article 3 (1) and (2) of these draft RTS are not met.

If you do not agree, clearly set out your rationale and provide supporting evidence where available.

Q2: Do you agree that the functions a CCP must always have are necessary to ensure that

- the CCP can ensure, on the appointing institutions' behalf, establishments' compliance with the host Member State's AML/CFT requirements?
- Facilitate supervision by the host Member State's competent authorities?

If you do not agree, please explain which functions you think the CCP should have, and why.

Q3: Do you agree that CCPs should be required to fulfil one or more of the additional functions in Article 6 of these draft RTS where this is commensurate to the ML/TF risk associated with the operation of establishments other than a branch on the host Member State's territory?

If you do not agree, clearly set out your rationale and provide supporting evidence where available. Please also set out whether you think that these additional functions should be core functions instead, and if so, why.

- Q4: What level of resource (financial and other) would be required to comply with these RTS? Please differentiate between one-off (set-up) costs and ongoing (running) costs. When providing your answer, please consider that the ESAs' mandate in Article 45(10) of Directive (EU) 2015/849 does not extend to determining the form a CCP should take.